PERIMETRY RESEARCH

Security barometer of .fr domains

How well are the active .fr domains protected? Passive measurements of a random sample of the domains in the .fr registry's open data, by age, mail provider and kind of site, compared with public bodies.

November 2026 edition

17,820
active domains measured

11.7%
enforce DMARC (quarantine or reject)

3%
get an A or a B

Perimetry Cloud
perimetry.cloud · Published 14 November 2026

About this report

Perimetry Research publishes studies of how well organisations protect their websites and e-mail, measured with the same passive checks as Perimetry Cloud. This edition covers a random sample of 20,000 domains drawn from the 4,633,263 .fr domains in the open data of Afnic, the .fr registry; 17,820 of them are active. The registry does not say who holds most .fr domains, and many belong to private persons: this report names no domain, and every figure is an aggregate.

Contents

01 Executive summary 3

02 Key findings 4

03 Grades 5

04 Check by check 6

05 By age of the domain 8

06 By mail provider 9

07 By kind of site 10

08 Compared with public bodies 11

09 Recommendations 12

10 Methodology 13

11 About Perimetry 15

01

Executive summary

17,820	32	11.7%	3%
active domains measured	average score out of 100	enforce DMARC (quarantine or reject)	get an A or a B

Average score of the 17,820 graded domains: 32 out of 100; median 33.

1. 71.6% of the graded domains have a strict SPF record and 38.6% publish a DMARC policy, but only 11.7% enforce it. For the others, an e-mail forged in their name (a fake invoice, a change of bank details) is generally delivered.
2. Websites: 59.1% of the domains with a site of their own have a valid certificate and 53.4% send visitors from HTTP to HTTPS; 17.3% use HSTS for six months or more and 14.1% send the basic protective headers.
3. 25.9% of the domains are signed with DNSSEC; 1.2% publish a CAA record.
4. Younger domains do better: 37 out of 100 on average for those registered less than two years ago, 27 for those registered more than ten years ago.
5. The mail provider matters: the domains whose mail is at Google Workspace average 39, at Microsoft 365 37, at OVHcloud 29.
6. Overall, 32 out of 100 on nine checks; the French communes average 47 on ten.

02

Key findings

What the active domains use

Mail provider



Microsoft 365 5.1% Google Workspace 3.8% OVHcloud 32% Another mail provider 45.5%
No mail server (no MX) 13.7%

Website



WordPress 17% A site builder (Wix, Shopify, Squarespace, Webflow, Jimdo) 4.4%
Another kind of site 60.5% No site of its own (mail only, or redirects to another domain) 18.1%

E-mail: DMARC rarely enforced

71.6% of the graded domains have a strict SPF record and 38.6% publish a DMARC policy, but only 11.7% enforce it. For the others, an e-mail forged in their name (a fake invoice, a change of bank details) is generally delivered.

Websites

Websites: 59.1% of the domains with a site of their own have a valid certificate and 53.4% send visitors from HTTP to HTTPS; 17.3% use HSTS for six months or more and 14.1% send the basic protective headers.

DNS

25.9% of the domains are signed with DNSSEC; 1.2% publish a CAA record.

Older domains lag behind

Younger domains do better: 37 out of 100 on average for those registered less than two years ago, 27 for those registered more than ten years ago.

The mail provider

The mail provider matters: the domains whose mail is at Google Workspace average 39, at Microsoft 365 37, at OVHcloud 29.

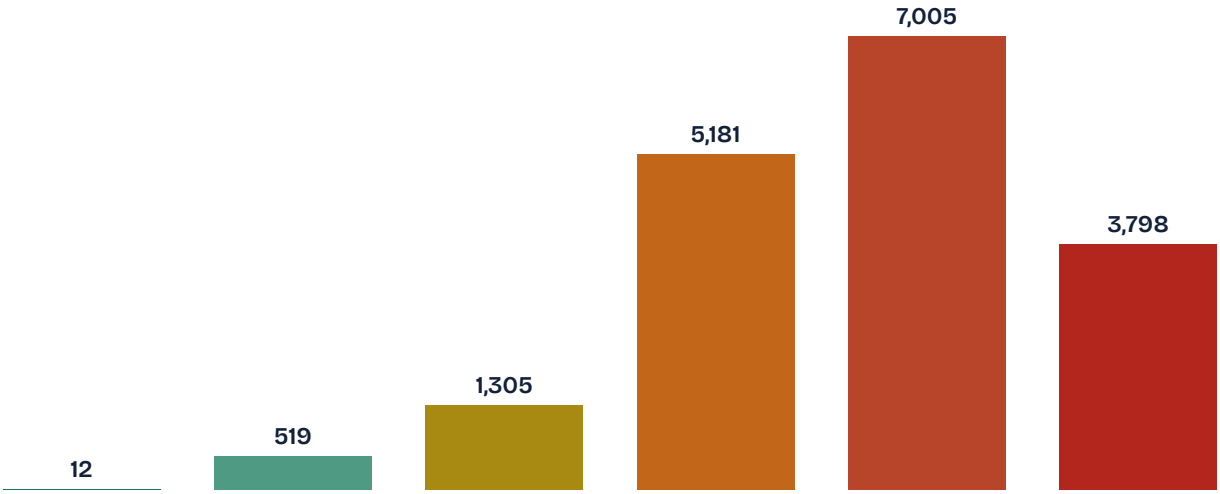
Compared with the communes

Overall, 32 out of 100 on nine checks; the French communes average 47 on ten.

03

Grades

Each active domain gets a score: the share of the nine checks that it passes, among those that apply to it (the score of our studies of public bodies, without the check on the contact address, which a domain alone does not give). Grades: A from 90, B from 75, C from 60, D from 40, E from 20, F below.



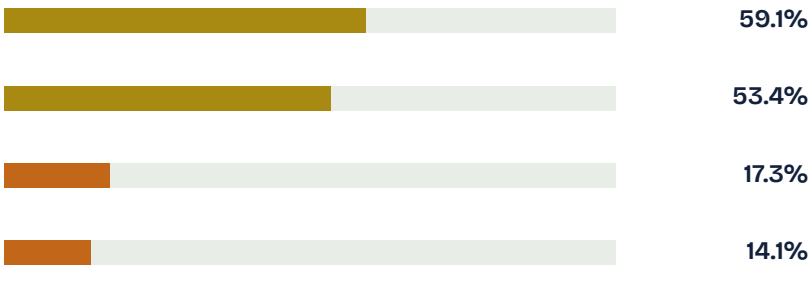
A: 12 (0.1%)
B: 519 (2.9%)
C: 1,305 (7.3%)
D: 5,181 (29.1%)
E: 7,005 (39.3%)
F: 3,798 (21.3%)

04

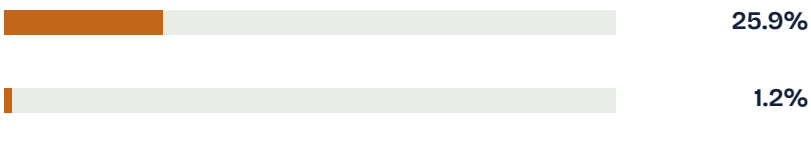
Check by check

Share of the graded domains that pass each check, among those it applies to. The website checks apply only to a domain with a site of its own.

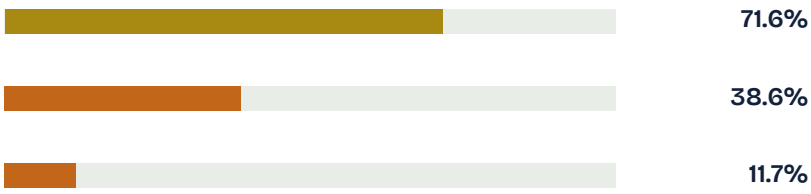
Website



DNS



E-mail



The nine checks	
Website · Valid HTTPS certificate	The site answers over HTTPS with a certificate that is in date, issued for its name, and trusted by browsers.
Website · HTTP sends visitors to HTTPS	Someone who types the address lands on the encrypted site, not on a page anyone on the network can read or alter.
Website · HSTS for six months or more	Browsers remember to use HTTPS only, so the first unencrypted request cannot be hijacked.
Website · Basic protective headers	X-Content-Type-Options: nosniff, and protection against being framed by another site (X-Frame-Options or CSP frame-ancestors).
DNS · DNSSEC	Answers about the domain are signed, so a resolver cannot be fed false addresses for its site or mail.
DNS · CAA record	The domain names the certificate authorities allowed to issue certificates for it.
E-mail · Strict SPF	The domain lists the servers allowed to send its mail and asks receivers to reject or flag the others (-all or ~all).

The nine checks	
E-mail · DMARC record	The domain publishes a DMARC policy, the standard that ties SPF and DKIM to the visible sender.
E-mail · DMARC enforced	The policy is quarantine or reject: messages forged in the domain's name, a fake invoice to a customer for example, go to spam or are refused, not delivered.

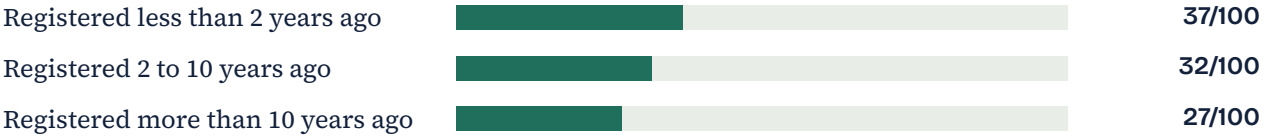
05

By age of the domain

From the creation date in the registry's file.

Group	Graded	Average	A or B	DMARC enforced	Median
Registered less than 2 years ago	5,705	37	4.3%	12.9%	33
Registered 2 to 10 years ago	7,704	32	2.5%	11%	33
Registered more than 10 years ago	4,411	27	2.2%	11.1%	22

Average



DMARC enforced



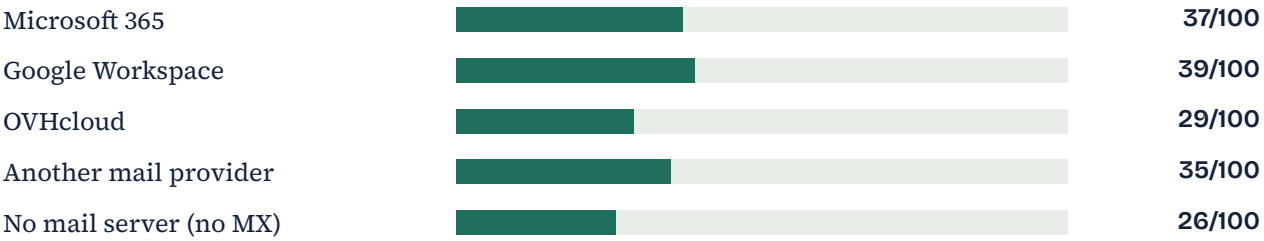
06

By mail provider

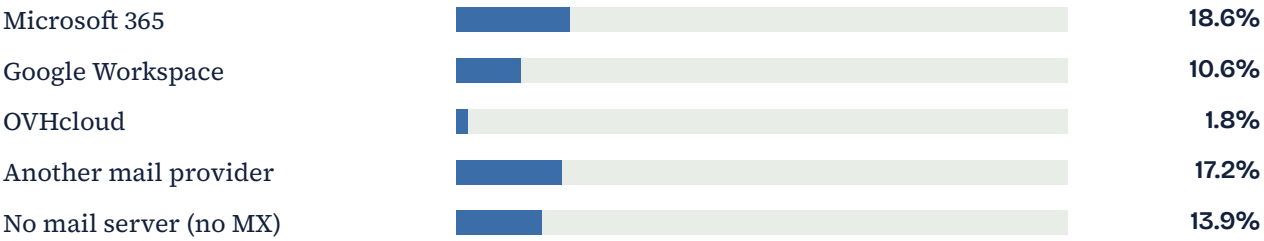
From the names of the domain's mail servers (MX). OVHcloud sets up its mail servers by default on many of the domains registered there: its group mixes mailboxes in use and settings left as they came.

Group	Share	Graded	Average	A or B	DMARC enforced	Median
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
Another mail provider	45.5%	8,108	35	3.5%	17.2%	33
No mail server (no MX)	13.7%	2,434	26	4.4%	13.9%	22

Average



DMARC enforced



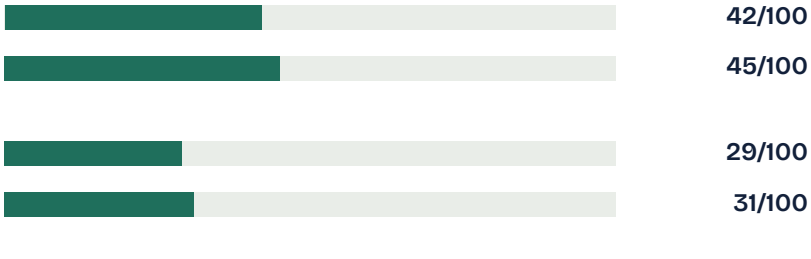
07

By kind of site

From the home page. A domain with no site of its own (mail only, or a site that sends visitors to another domain) is judged on its DNS and mail only.

Group	Share	Graded	Average	A or B	DMARC enforced	Median
WordPress	17%	3,030	42	2.6%	7.9%	44
A site builder (Wix, Shopify, Squarespace, Webflow, Jimdo)	4.4%	782	45	4.3%	6.1%	44
Another kind of site	60.5%	10,790	29	2.1%	10.2%	22
No site of its own (mail only, or redirects to another domain)	18.1%	3,218	31	5.9%	21.5%	20

Average



DMARC enforced



08

Compared with public bodies

The same checks as our studies of the French communes, local authorities and higher education establishments (latest editions): share of the graded bodies that pass each one. Their averages count ten checks for the communes and local authorities, nine for higher education and the .fr domains.

	Communes	Local authorities	Higher education	.fr domains
Average score	47	60	64	32
Valid HTTPS certificate	93.4%	98.7%	100%	59.1%
HTTP sends visitors to HTTPS	86.4%	90.9%	95.2%	53.4%
HSTS for six months or more	28.3%	38.8%	46.1%	17.3%
Basic protective headers	26.1%	40.7%	57.5%	14.1%
DNSSEC	22.1%	25.9%	12.7%	25.9%
CAA record	2.8%	2.6%	41%	1.2%
Strict SPF	85.9%	97.1%	93%	71.6%
DMARC record	45.2%	77.8%	86.9%	38.6%
DMARC enforced	19.2%	32.8%	45.4%	11.7%

09

Recommendations

1 Enforce DMARC

Publishing a DMARC policy is not enough: read its reports for a few weeks, list every service that sends in your name (invoicing, newsletter, online shop), then move to quarantine and reject. That is what stops an e-mail forged in your name from reaching your customers.

2 Redirect to HTTPS and turn on HSTS

Every visit should land on the encrypted site; HSTS makes browsers remember it. Most hosts and site builders offer both in a setting.

3 Sign your domain with DNSSEC and add a CAA record

Most registrars offer DNSSEC, often in one click. A CAA record lists the authorities allowed to issue your certificates.

4 Review old settings

The older a domain, the lower its score: records set up years ago (a former mail provider in SPF, a site no one updates) are rarely revisited.

5 Watch it over time

Certificates expire, providers change, records get lost in a migration. A regular check catches it before your customers do.

10

Methodology

Passive checks only

We read what any visitor or mail server can see: public DNS records, the domain registration (RDAP), the TLS certificate, one request for the home page over HTTP (its redirect is read, not followed), and the home page over HTTPS (following its redirects, as a browser would). Nothing else on the site is requested. When a domain publishes an MTA-STS policy, its policy file is read too, as mail servers do.

No port scanning, no subdomain discovery, no login attempts, no forms, no testing for vulnerabilities. The robot is slow on purpose and spreads its requests over several hours.

The robot

It identifies itself as PerimetryResearch/1.0 (+https://perimetry.cloud/research/methodology/). If you run a site it visited and would rather it did not, write to hello@perimetry.cloud and we will leave the domain out of the next editions.

The study of active .fr domains

Population: the .fr domains in the open data of Afnic, the .fr registry (file A, “Noms de domaine en .fr”, Licence Ouverte), that are still registered, plain .fr (not asso.fr, com.fr and the like) and not internationalised. The file gives the holder’s type for very few domains, the holders’ data being protected: the few marked as held by a natural person, or by a holder outside France, are left out; all the others are kept. The November 2026 edition draws on the file of September 2026: 4,633,263 eligible domains.

A random sample of 20,000 of them is measured, drawn again identically from the edition’s seed. With a sample this size, a share measured on all of it is within about one point of the share among all eligible domains (95% confidence); for a group, the margin grows as the group gets smaller.

Because the holder is unknown for most domains, the study cannot tell a company’s domain from an association’s or a private person’s. That is why it never names a domain, not even the good performers: it publishes aggregates only.

A domain is inactive, counted and left out, when it does not exist in DNS or has neither a site in use nor a mail server: a parked page or a host’s placeholder page is not a site in use. The site is read on the domain itself, then on www when the domain itself has no site. A domain whose site sends visitors to another domain (an alias of a brand’s main address, for example) is judged on its DNS and mail only, its site being someone else’s.

The checks, score and grades of the communes study, without the check on the contact address, which a domain alone does not give: nine checks, as in the study of higher education. A domain needs three checks that apply to be graded.

Groups: by age (from the creation date in Afnic’s file), by mail provider (from the names of the mail servers, MX, of the domain: Microsoft 365, Google Workspace, OVHcloud, another provider, none) and by

kind of site (from the home page: WordPress, a site builder, another kind of site, none of its own). OVHcloud sets up its mail servers by default with many of the domains registered there: its group mixes mailboxes in use and settings left as they came. The registrars are not published.

Limits

Each edition is a snapshot taken over a few hours. The directory can be out of date or wrong; we use it as published. DKIM keys are looked for on common selectors only, so they are not graded. A site behind a protection service may answer differently to a robot than to a visitor. Mail servers are not tested (STARTTLS needs port 25, which the study's infrastructure cannot reach).

11

About Perimetry

Perimetry is an open source tool that audits the outside of a domain the way anyone on the internet sees it: e-mail authentication, DNS, certificates, mail servers, websites. Perimetry Cloud is its hosted version, with continuous monitoring, alerts and reports, for organisations and the agencies that look after them.

Cite as: Perimetry Research, Security barometer of .fr domains, November 2026. https://perimetry.cloud/research/fr-domains/

You may reuse the figures of this report with a link to the study. Afnic's open data remain under the Licence Ouverte (source: Afnic, file A of the .fr domains).

Contact: hello@perimetry.cloud

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