INTRAGREAT CONSULTING · DMARC MONITORING

Email Domain Protection Report

Example Company · example.com

October 2026

Generated November 6, 2026

SAMPLE REPORT — generated from demonstration data, not real traffic.

MESSAGES REPORTED	PASSED DMARC	SPOOFING ATTEMPTS	STOPPED BY RECEIVERS
25,646	**97.1%**	**386**	**671**
+5% vs last month	+2.1 pts vs last month	+30% vs last month	355 rejected · 316 quarantined

`p=quarantine` **Partially protected.** Spoofed mail is sent to junk folders, where recipients can still find and act on it. We recommend moving to **p=reject**.

Recommended actions

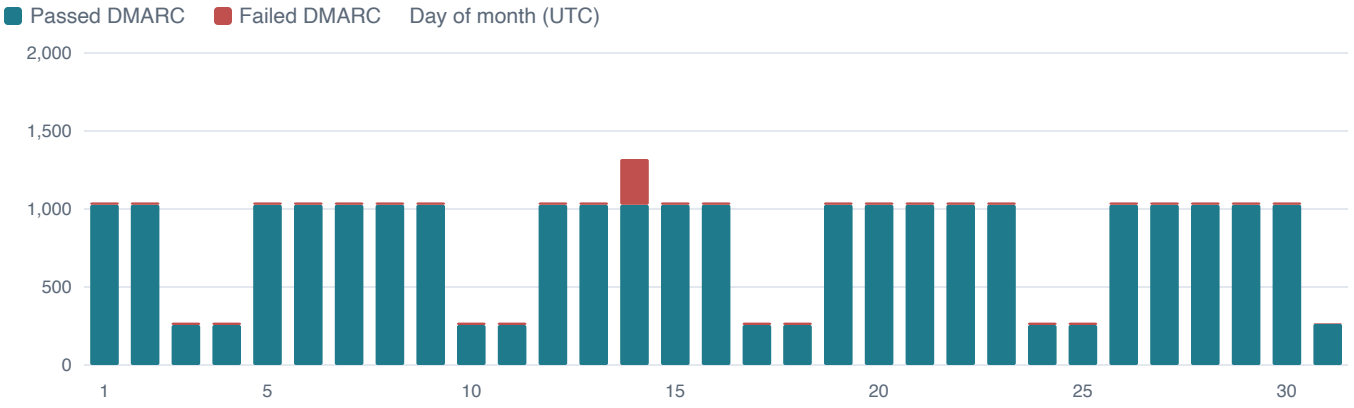
example.com is at p=quarantine — recommend p=reject
Quarantined spoofs still land in recipients' junk folders, where they get opened. With senders authenticating cleanly, reject is the recommended end state.

Billing system is failing authentication (316 of 412 messages)
This is a sender you use. Fix SPF alignment and DKIM signing so its mail isn't blocked once the policy is enforced.

New authenticated sender: Help desk software (188 messages)
This service is sending as your domain and passing DMARC, but it isn't on your approved list. Confirm it's yours — if not, revoke its access.

31 unauthorized messages were still delivered
Receivers delivered these because the policy wasn't enforcing. Moving to p=reject stops them.

Daily volume



Who is sending as your domain

SOURCE	MESSAGES	DMARC PASS	SPF ALIGNED	DKIM ALIGNED	STATUS
Microsoft 365 14 IPs	18,420	100%	100%	100%	Authenticated
Marketing email platform 6 IPs	6,240	100%	0%	100%	Authenticated
Billing system 2 IPs	412	23%	23%	0%	Approved sender failing
Help desk software 3 IPs	188	100%	0%	100%	Authenticated (unlisted)
Unidentified senders 9 IPs · no reverse DNS — see impersonation attempts	386	0%	0%	0%	Unauthorized

Impersonation attempts

COUNTRY	MESSAGES	IPS
Example A	164	4
Example B	121	3
Example C	101	2

TOP SOURCE IPS	MESSAGES	OUTCOME
203.0.113.24 (Example A)	164	reject / quarantine
198.51.100.77 (Example B)	121	reject / none
192.0.2.140 (Example C)	101	reject

Outcome is what the receiving server did: **reject** = refused, **quarantine** = junk folder, **none** = delivered.

Reporting mail providers

PROVIDER	REPORTS	MESSAGES COVERED
Google	31	15,120
Microsoft	31	8,874
Yahoo	29	1,652

How to read this report

DMARC tells receiving mail servers what to do with mail that claims to be from your domain but can't prove it. Providers like Google and Microsoft send daily reports back to Intragreat Consulting; this report summarizes them.

Authenticated — passed DMARC from a service you've approved. **Authenticated (unlisted)** — passed, but from a service not yet on your approved list. **Approved sender failing** — a service you use is misconfigured and its mail may be junked or blocked. **Unauthorized** — failed authentication from a source you don't use: spoofing, or mail forwarded through another server.

Reports describe traffic seen by participating providers (most major mailbox providers). Small or private mail systems may not report. Times are UTC.