GUARDIAN360

in partnership with DMARC Advisor

Email Security Benchmark

DMARC protection among Managed Service Providers in the DACH region

Germany · Austria · Switzerland | 1,311 providers scanned

NETWORKING EVENT

Cross-border Cybersecurity Networking Event for MSPs and IT system houses

TopGolf Oberhausen · 2 September 2026

Data analysis by DMARC Advisor | Report by Guardian360 · July 2026 · benchmark data collected 8 July 2026

Organised by the Netherlands government & InnovationQuarter, with Passguard, SecuMailer, SecureMe2, DMARC Advisor and Guardian360.

Executive summary

Email remains the number one channel through which organisations are attacked. DMARC (Domain-based Message Authentication, Reporting and Conformance) is the single most effective control an organisation can deploy to stop criminals from sending email in its name. Yet adoption at an *enforcing* level remains strikingly low, even among the very companies that sell security for a living.

This benchmark was produced for the Cross-border Cybersecurity Networking Event for MSPs and IT system houses (TopGolf Oberhausen, 2 September 2026). **DMARC Advisor** analysed the public DMARC configuration of **1,311 Managed Service Providers (MSPs)** across Germany, Austria and Switzerland, and **Guardian360** produced this report on the findings. Applying a strict definition in which only a policy of **p=reject** counts as protected, the results are sobering.

74.5%

of DACH MSPs are NOT protected against email spoofing

Only **25.5%** of the MSPs scanned enforce DMARC with p=reject. The remaining three quarters either publish no DMARC record at all, or run a policy (p=none or p=quarantine) that still allows spoofed mail to reach the recipient, either in the inbox or in the spam folder that most users actively check. Because MSPs manage email and IT for thousands of downstream customers, an unprotected MSP domain is not only a risk to that provider, but a credible attack path into its entire client base.

Key findings at a glance

- **Only 1 in 4 is protected.** 334 of 1,311 MSPs (25.5%) enforce p=reject. The largest single group, 398 providers (30.4%), sit on p=quarantine, which does not stop spoofing.
- **Nearly 1 in 5 has no DMARC record at all.** 257 providers (19.6%) publish no DMARC record whatsoever, leaving their domain fully open to impersonation.
- **Remarkably consistent across borders.** Protection sits at 27.7% in Switzerland, 25.2% in Germany and 22.4% in Austria. This is a structural gap, not a national one.
- **Size barely helps.** Large and enterprise MSPs are only marginally better protected than one-person shops. Even in the best-performing size band, fewer than a third are protected.
- **The specialist paradox.** MSPs that explicitly sell Cybersecurity or Email Security services (26.4% protected) barely outperform the overall average and fail to protect their own domain in almost three out of four cases.
- **Reporting is a blind spot.** 42.0% of MSPs have no DMARC aggregate reporting (RUA) configured at all, meaning they have zero visibility into who is sending mail in their name.

Scope, method and definitions

The benchmark is based on an external, non-intrusive scan of publicly available DNS records. No systems were accessed and no data beyond public DMARC and DNS information was collected. The dataset comprises **1,311 MSPs** listed for the DACH region: 1,006 in Germany, 220 in Switzerland and 85 in Austria. For each domain the published DMARC record was retrieved, the enforcement policy classified, and the presence of aggregate reporting (rua) checked.

About this report and the event

This report is released in the context of the **Cross-border Cybersecurity Networking Event for MSPs and IT system houses**, held at TopGolf Oberhausen on 2 September 2026. The event is organised by the Netherlands government (its diplomatic network in Germany) together with the regional development agency InnovationQuarter, and brings German MSPs together with five Dutch cybersecurity companies: Passguard, SecuMailer, SecureMe2, DMARC Advisor and Guardian360. The data analysis behind this benchmark was performed by **DMARC Advisor**; the report was produced by **Guardian360**. Because the event primarily brings together MSPs from Nordrhein-Westfalen, the regional findings for NRW (see the spotlight later in this report) are of particular relevance to its audience.

How we classify protection

Following the classification agreed with DMARC Advisor, every domain is reduced to a binary outcome: **Protected** or **Not Protected**. The logic is deliberately strict, because anything short of full enforcement still allows a spoofed message to reach the recipient.

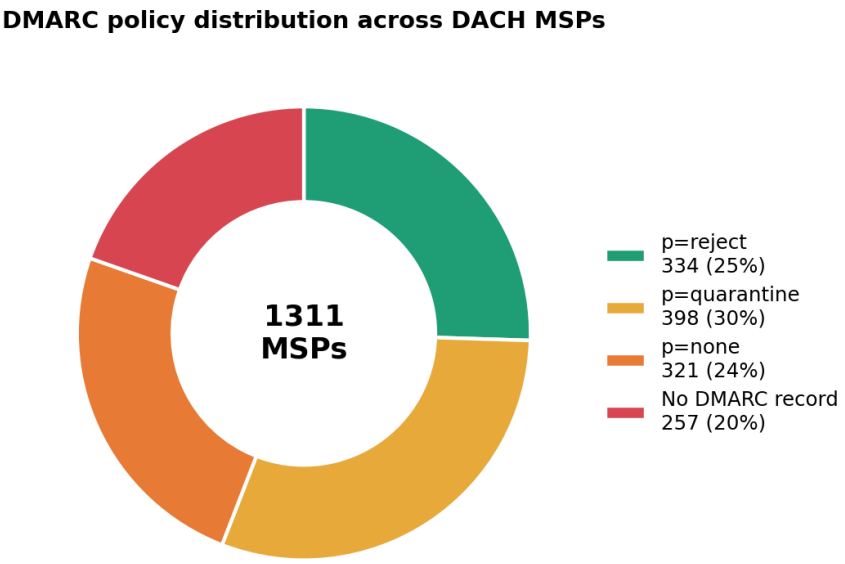
Status	Criterion	What it means
Protected	p=reject only	The domain is fully protected. Spoofed mail is rejected outright before delivery.
Not Protected	p=quarantine	Spoofed mail is not blocked; it is routed to spam/junk, where 76-86% of users still look for 'lost' mail.
Not Protected	p=none	Monitoring only. No enforcement or blocking takes place; spoofing succeeds.
Not Protected	No DMARC record	No record published. The domain is completely open to impersonation.

The rationale is simple: with No DMARC, p=none *and* p=quarantine, a spoofed email still successfully arrives at the recipient. Because the average user actively checks their spam folder for legitimate mail, they remain highly vulnerable. Only p=reject removes the message before it can do harm. This is why we do not count p=quarantine, the single largest group in this dataset, as protected.

> *A note on p=reject: organisations should never move straight to p=reject. Monitor RUA reports first, confirm every legitimate sender authenticates correctly, then tighten the policy. Enforcing prematurely can block legitimate business mail.*

The overall picture

Across all 1,311 MSPs, the four DMARC states are spread almost evenly, with p=quarantine, a policy that offers a false sense of security, being the most common configuration of all.

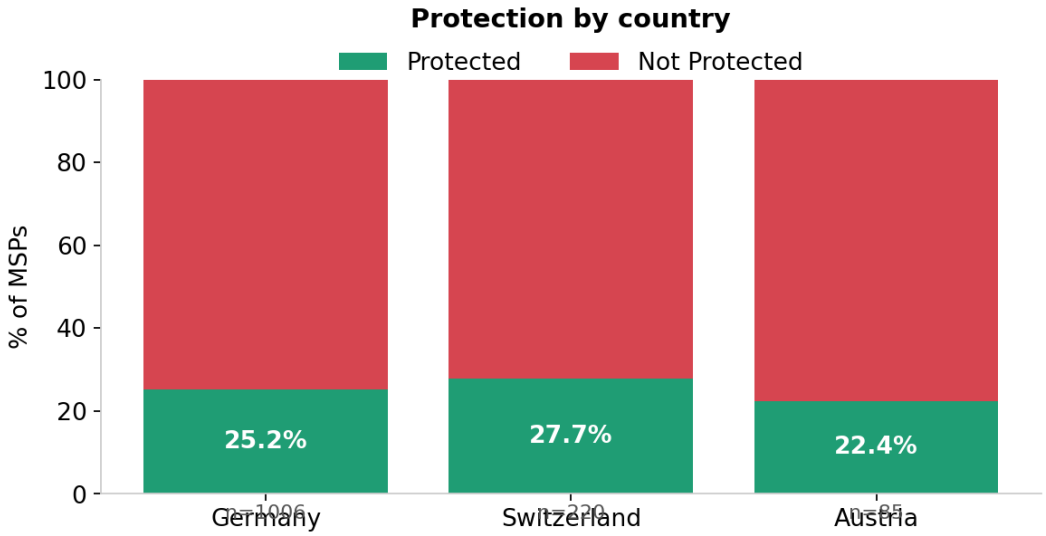


DMARC policy	MSPs	Share	Protected?
p=reject	334	25.5%	Protected
p=quarantine	398	30.4%	Not Protected
p=none	321	24.5%	Not Protected
No DMARC record	257	19.6%	Not Protected
Total scanned	1,311	100%	-

Reduced to the binary that matters, **977 of the 1,311 providers scanned (74.5%) are not protected** against having email sent in their name. For a sector whose entire proposition rests on being a trusted, secure extension of its customers' IT, this is a significant exposure.

Analysis by country

One might expect meaningful differences between the three markets. In practice the picture is strikingly uniform: protection ranges only from 22.4% to 27.7%. The problem is structural across the German-speaking region rather than specific to any one country.



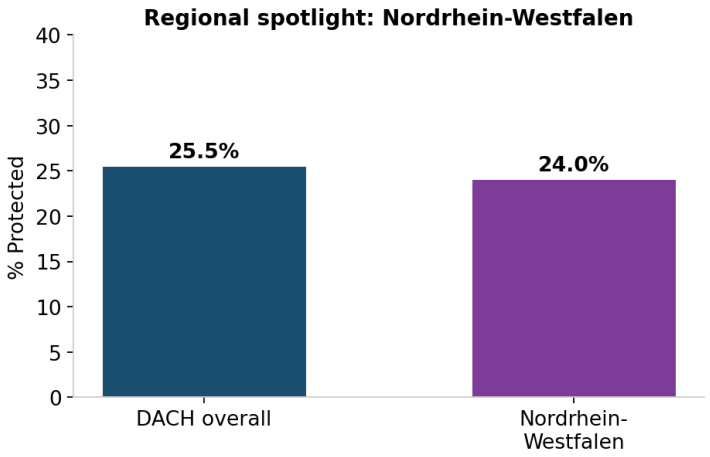
Country	MSPs	p=reject	quarantine	p=none	No record	% Protected
Germany	1,006	254	296	243	212	25.2%
Switzerland	220	61	74	52	33	27.7%
Austria	85	19	28	26	12	22.4%

Switzerland leads narrowly at **27.7%**, followed by Germany (**25.2%**) and Austria (**22.4%**). Austria also has the highest share of providers stuck on p=none (monitoring only), suggesting a number of organisations have started the DMARC journey but never completed it.

Regional spotlight: Nordrhein-Westfalen

As Germany's most populous state and densest MSP market, Nordrhein-Westfalen (NRW) was analysed separately. With **221 providers**, NRW tracks the DACH average almost exactly, confirming that even in a mature, competitive regional market the enforcement gap persists.

This region is especially relevant here: the networking event itself takes place in Oberhausen, in the heart of NRW, and its audience consists largely of MSPs and IT system houses from the region. The figures below therefore describe the immediate peer group of most attendees, and a fair yardstick against which each can measure its own domain.



Metric	Nordrhein-Westfalen	DACH overall
MSPs analysed	221	1,311
p=reject (Protected)	53 (24.0%)	334 (25.5%)
p=quarantine	67	398
p=none	55	321
No DMARC record	46	257
Not Protected	168 (76.0%)	977 (74.5%)

In NRW, 76.0% of MSPs are not protected, virtually identical to the region-wide 74.5%. The single largest group, again, is p=quarantine.

Protection by German federal state

Within Germany, protection rates vary more at state level, though small sample sizes in the least populous states warrant caution. The larger MSP markets cluster tightly around the national average.

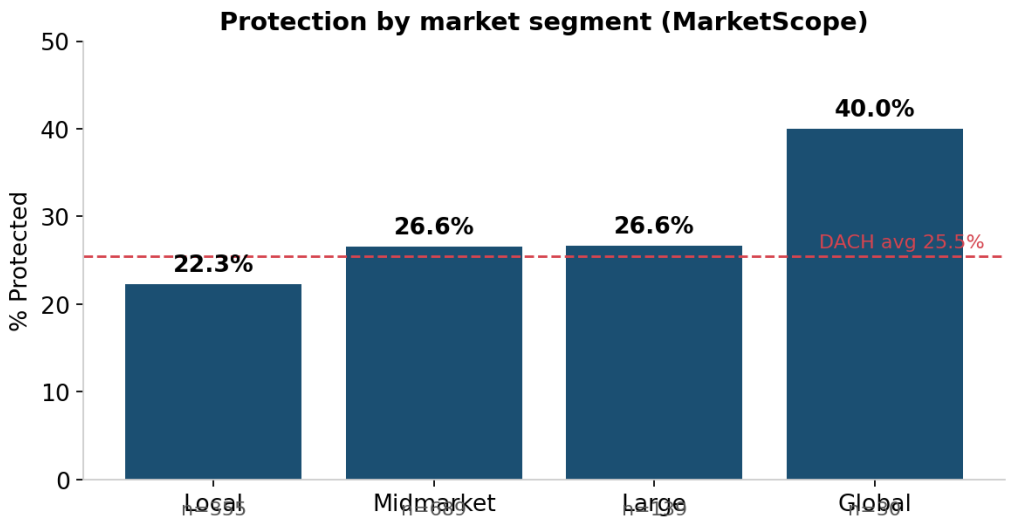
Federal state	MSPs	Protected	% Protected
Nordrhein-Westfalen	221	53	24.0%
Bayern	194	54	27.8%
Baden-Württemberg	141	30	21.3%
Hessen	96	22	22.9%
Niedersachsen	66	17	25.8%
Berlin	57	14	24.6%
Hamburg	53	12	22.6%
Rheinland-Pfalz	44	13	29.5%
Schleswig-Holstein	36	6	16.7%

> *States with fewer than 30 MSPs omitted for statistical reliability.*

Analysis by company type and size

By market segment

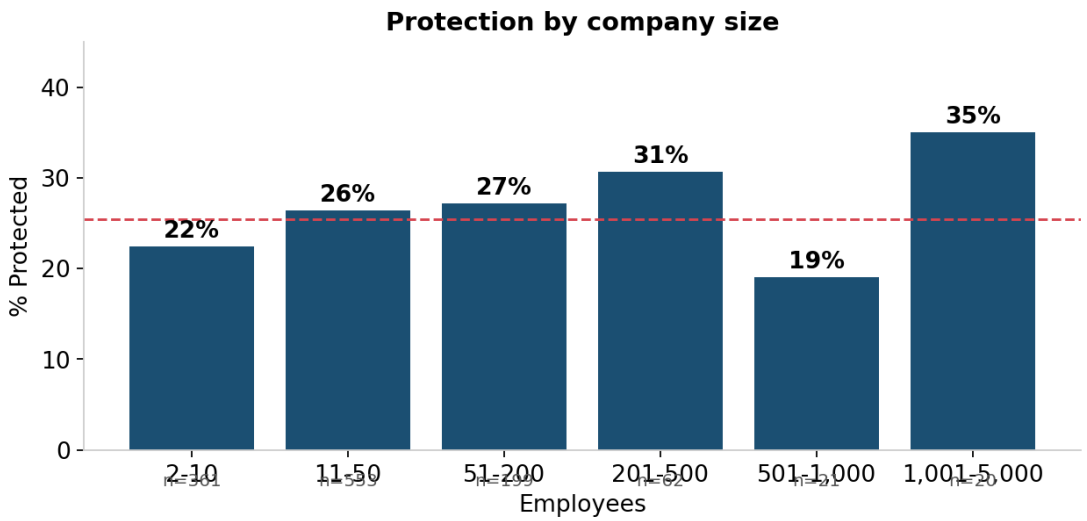
Classifying MSPs by the market they primarily serve (MarketScope) shows that only the small group of globally operating providers meaningfully beats the average. Local providers, the most numerous group serving SMEs, are the least protected.



Market segment	MSPs	% Protected
Local	355	22.3%
Midmarket	689	26.6%
Large	139	26.6%
Global	30	40.0%

By company size

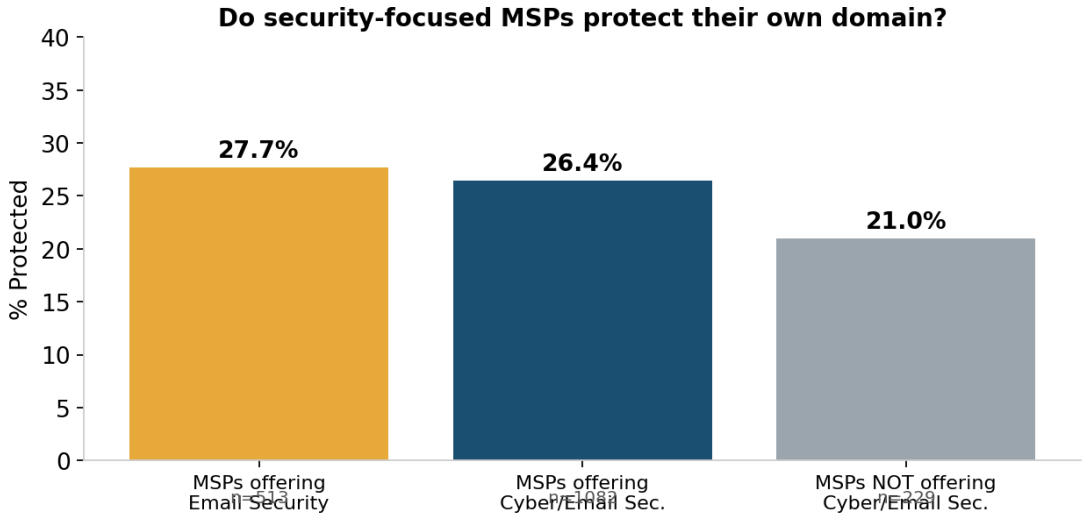
The intuition that bigger, better-resourced providers are better protected only weakly holds. Protection creeps up modestly with size in the mid-range, but even the best-performing bands leave roughly two-thirds of providers exposed, and the very largest categories are inconsistent due to small numbers.



The takeaway is uncomfortable but clear: DMARC enforcement is not primarily a resourcing problem. Providers of every size are failing to close a gap that is free to fix and squarely within their own expertise.

The specialist paradox

Perhaps the most telling cut of the data compares MSPs by what they sell. If any group should have its own house in order, it is the providers that explicitly market **Cybersecurity** and **Email Security** services to their customers.

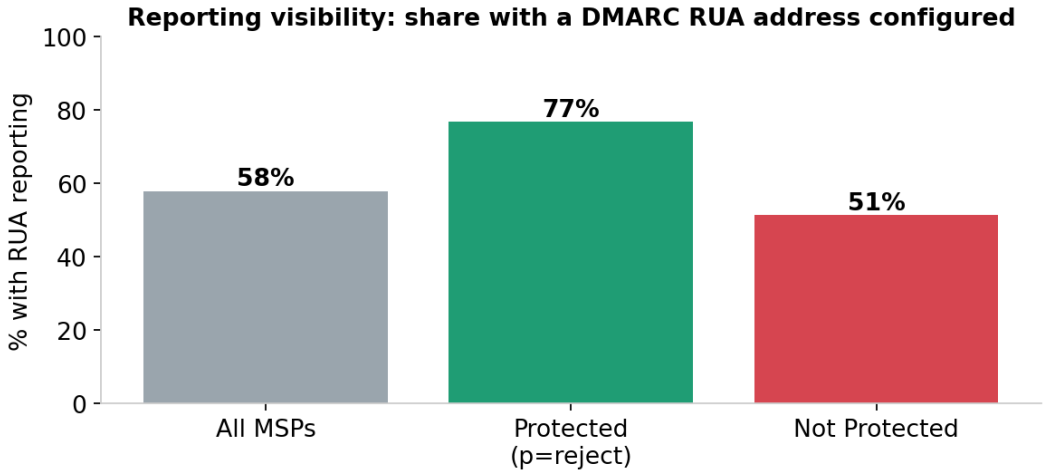


Group	MSPs	% Protected
MSPs offering Email Security	513	27.7%
MSPs offering Cyber/Email Security	1,082	26.4%
MSPs NOT offering either	229	21.0%

Security specialists do protect themselves slightly more often, but the difference is marginal: **26.4% versus 21%**. Put plainly, roughly **three out of four MSPs that sell email security cannot demonstrate that their own domain is protected against spoofing.** For prospective customers and partners, this is a straightforward and fair due-diligence question to ask.

Reporting and visibility (RUA)

A DMARC policy is only half the story. The aggregate reporting address (rua) is what gives an organisation visibility into who is sending mail in its name, which legitimate services need authenticating, and where spoofing attempts originate. Without it, an organisation is flying blind, and cannot safely progress towards p=reject.



Group	% with RUA reporting configured
All MSPs	58.0%
Protected (p=reject)	76.9%
Not Protected	51.5%

42.0% of all MSPs have no reporting configured at all. Reporting correlates strongly with enforcement: 76.9% of protected providers collect RUA data, versus only 51.5% of unprotected ones, which is exactly the sequence a healthy DMARC rollout follows: turn on reporting, learn, then enforce.

> *Important nuance: an external scan can confirm that a rua address exists, but not whether anyone actually reads the reports. When reports are delivered to an internal mailbox they arrive as raw XML, which is time-consuming and error-prone to interpret, and are frequently archived unread. Establishing clear ownership of the DMARC protocol, ideally with automated report processing, is essential.*

What this means, and what to do

The headline of this benchmark is not that DMARC is hard. It is that a control which is free, well-documented and directly within the expertise of every MSP is left unfinished by three quarters of the sector. For MSPs specifically, the stakes are amplified: an unprotected provider domain is a ready-made template for attackers to impersonate a trusted supplier to its own customers.

For MSPs

- **Publish a DMARC record today if you have none.** Start at p=none with a reporting address so you gain visibility without risk.
- **Do not stop at p=quarantine.** It is the most common configuration in this dataset and it does not protect you. Treat it as a waypoint, not a destination.
- **Read your RUA reports.** Use them to identify and authenticate every legitimate sender, then move deliberately to p=reject.
- **Practise what you sell.** If you offer email or cyber security, a protected domain is the minimum credible proof point.

For customers and partners

- **Ask the question.** "Is your primary domain on DMARC p=reject, and do you monitor RUA?" is a fair, revealing due-diligence question for any provider.
- **Check your own posture too.** The same strict test applies to your organisation's domains.

How Guardian360 and DMARC Advisor help

Guardian360 and DMARC Advisor help organisations move safely from no protection to full enforcement: continuous scanning and monitoring, automated interpretation of RUA reports, and expert guidance to reach p=reject without disrupting legitimate mail. Both take part in the Cross-border Cybersecurity Networking Event alongside Passguard, SecuMailer and SecureMe2. The goal of this benchmark is not to name and shame, but to make an invisible risk visible, and to help the sector, and the MSPs in the room, close a gap they are uniquely well placed to close.

About this benchmark. Data analysis by DMARC Advisor; report produced by Guardian360. Based on a non-intrusive external scan of public DNS/DMARC records for 1,311 DACH MSPs, data collected 8 July 2026. Prepared for the Cross-border Cybersecurity Networking Event for MSPs and IT system houses (TopGolf Oberhausen, 2 September 2026), organised by the Netherlands government and InnovationQuarter, with participating companies Passguard, SecuMailer, SecureMe2, DMARC Advisor and Guardian360. Percentages are rounded to one decimal place. A domain is classified Protected only when its DMARC policy is p=reject.