DMARCPULSE.IO

DACH Email Security Adoption Report 2026

An analysis of SPF, DMARC, MTA-STS and DNSSEC adoption across 503 domains in Germany, Austria and Switzerland

97.0%	87.3%	56.3%	8.2%
SPF Adoption	DMARC Adoption	DMARC Enforcement	MTA-STS Adoption

Published by DMARCPulse — April 2026
https://dmarcpulse.io

503 domains • 16 industries • 3 countries

Table of Contents

1. Executive Summary

This report analyzes the email authentication posture of **503 domains** across **Germany (327)**, **Austria (77)**, and **Switzerland (99)**, spanning 16 industries including government, education, banking, healthcare, technology, and more. All data was collected via public DNS queries in April 2026.

The DACH region shows strong foundational adoption: **97.0% of domains have SPF** and **87.3% have a DMARC record**. However, a critical enforcement gap persists: **only 56.3% actively enforce their DMARC policy** (quarantine or reject). Nearly a third of all domains with DMARC remain in monitoring mode (p=none), providing visibility but zero protection against domain spoofing.

Advanced protocols show even lower adoption. **MTA-STS, which enforces encrypted email transport, is deployed by just 8.2% of domains**. DNSSEC, which protects against DNS hijacking, reaches only 15.7%. These gaps leave the vast majority of DACH organizations vulnerable to man-in-the-middle attacks and DNS spoofing.

Switzerland leads the region in DMARC enforcement at **73.7%**, while Austria trails at **45.5%**. The education sector has the widest enforcement gap: 87.7% DMARC adoption but only 26.2% enforcement. Government domains fare similarly poorly, with 77.1% adoption but only 42.9% enforcement.

Key Finding	Value
Domains analyzed	503 (DE: 327, AT: 77, CH: 99)
SPF adoption	97.0%
DMARC adoption	87.3%
DMARC at p=reject (full protection)	36.2%
DMARC enforcement (quarantine + reject)	56.3%
DMARC at p=none (monitoring only)	31.0%
No DMARC record at all	12.7%
MTA-STS adoption	8.2%
DNSSEC adoption	15.7%

2. Methodology

The domain list was compiled from public sources including major stock indices (DAX 40, MDAX, SDAX, TecDAX, ATX, SMI), government websites at federal, state, and municipal levels, leading universities and research institutions, major hospitals and health insurers, national media outlets, and large private companies.

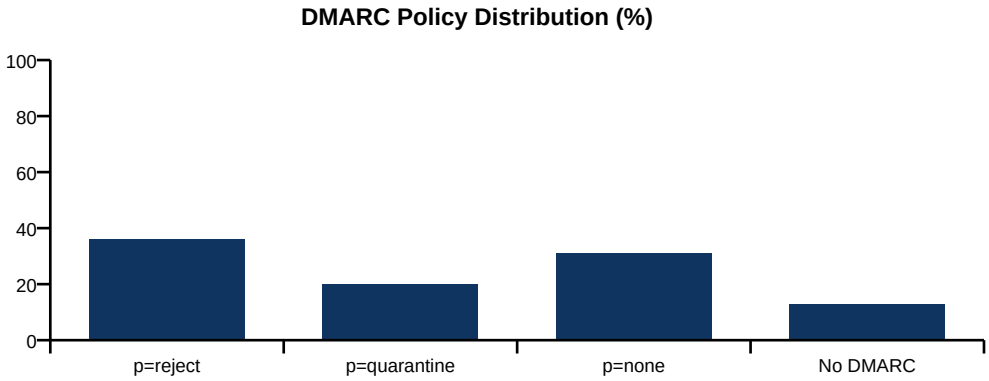
For each domain, four DNS-based checks were performed:

Protocol	DNS Query	What It Shows
SPF	TXT record on root domain	Which servers may send email for the domain
DMARC	TXT on _dmarc.domain	Policy for handling unauthenticated email (none/quarantine/reject)
MTA-STS	TXT on _mta-sts.domain	Whether inbound email transport encryption is enforced
DNSSEC	DNSKEY records	Whether the domain's DNS is cryptographically signed

All queries used public DNS resolvers (Google 8.8.8.8, Cloudflare 1.1.1.1). Data was collected on April 9, 2026. Only publicly observable DNS records were analyzed; no emails were sent and no private systems were accessed.

3. Overall Findings

Across all 503 DACH domains, SPF adoption is near-universal at 97.0%. DMARC adoption is high at 87.3%, but the enforcement picture is significantly weaker. Only 36.2% of domains enforce the strictest policy (p=reject), while 31.0% remain in monitoring mode (p=none) and 12.7% have no DMARC record at all.



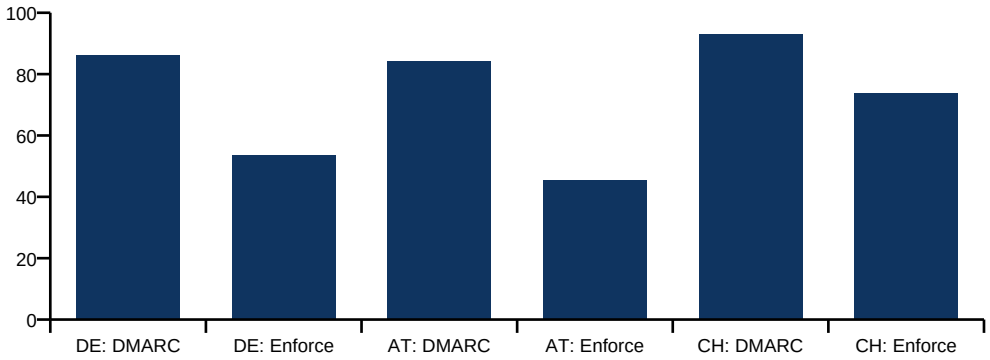
Metric	Count	Percentage
SPF record present	488	97.0%
DMARC record present	439	87.3%
DMARC p=reject	182	36.2%
DMARC p=quarantine	101	20.1%
DMARC p=none	156	31.0%
No DMARC record	64	12.7%
MTA-STS enabled	41	8.2%
DNSSEC enabled	79	15.7%

4. Country Comparison

Switzerland leads in nearly every metric. With 73.7% DMARC enforcement, it significantly outperforms Germany (53.5%) and Austria (45.5%). Switzerland also has the highest DMARC adoption rate (92.9%) and the lowest share of domains without any DMARC record (7.1%).

Austria shows the weakest posture overall, with 45.5% enforcement and 5.2% MTA-STS adoption. Germany sits in the middle but notably leads in MTA-STS deployment at 9.8%.

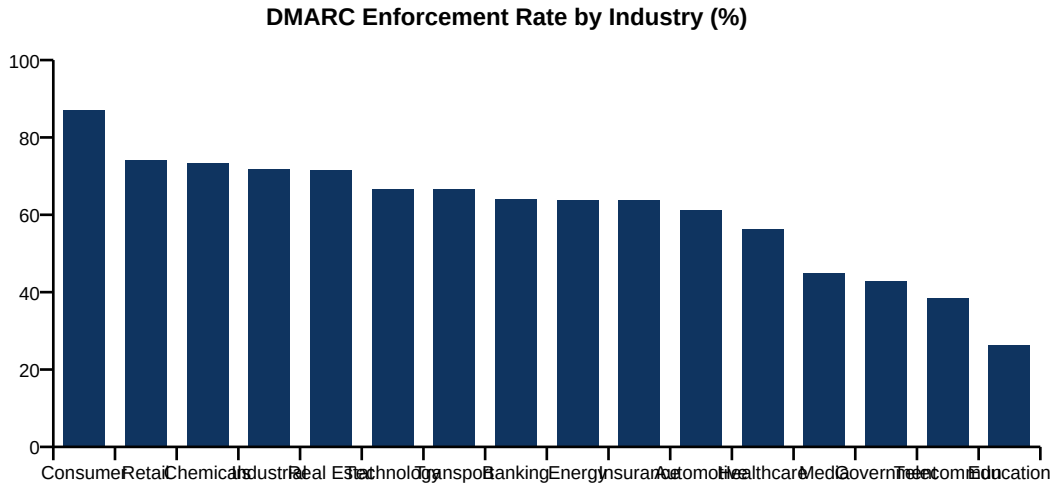
DMARC Adoption vs. Enforcement by Country (%)



Metric	Germany (327)	Austria (77)	Switzerland (99)
SPF	96.9%	94.8%	99.0%
DMARC	86.2%	84.4%	92.9%
p=reject	36.1%	27.3%	43.4%
p=quarantine	17.4%	18.2%	30.3%
p=none	32.7%	39.0%	19.2%
No DMARC	13.8%	15.6%	7.1%
MTA-STS	9.8%	5.2%	5.1%
DNSSEC	14.7%	14.3%	20.2%

5. Industry Breakdown

Industry-level data reveals stark contrasts. Consumer brands and retail companies lead in enforcement, driven by deliverability requirements from Google, Yahoo, and Microsoft. Education and government sectors lag significantly behind, despite handling sensitive data and being frequent targets of phishing campaigns.



Industry	N	SPF	DMARC	Enforce	p=reject	p=none	MTA-STS	DNSSEC
Consumer	23	100%	96%	87%	57%	9%	4%	13%
Retail	27	100%	100%	74%	56%	26%	11%	15%
Chemicals	15	100%	87%	73%	67%	13%	33%	0%
Industrials	53	100%	91%	72%	49%	19%	8%	11%
Real Estate	7	100%	100%	71%	57%	29%	14%	29%
Technology	33	91%	88%	67%	39%	21%	9%	12%
Transport	24	100%	79%	67%	58%	12%	8%	17%
Banking	25	96%	84%	64%	56%	20%	4%	16%
Energy	22	91%	86%	64%	50%	23%	14%	5%
Insurance	22	100%	91%	64%	36%	27%	5%	18%
Automotive	18	100%	89%	61%	39%	28%	6%	6%
Healthcare	48	92%	83%	56%	40%	27%	15%	10%
Media	38	97%	92%	45%	21%	47%	0%	8%
Government	70	97%	77%	43%	21%	34%	4%	20%
Telecommunications	13	92%	92%	38%	0%	54%	15%	15%
Education	65	98%	88%	26%	8%	62%	6%	34%

Key observations by industry:

• **Consumer & Retail** lead with 87% and 74% enforcement respectively. Bulk sender requirements from Google and Yahoo are clearly driving adoption.

• **Education** has the widest enforcement gap: 88% DMARC adoption but only 26% enforcement. 62% of university domains remain at p=none.

• **Government** shows similar weakness: 77% adoption, 43% enforcement. 23% of government domains have no DMARC at all.

• **Telecommunications** is the only sector with 0% p=reject adoption, despite 92% DMARC presence.

• **Chemicals** leads MTA-STS adoption at 33%. **Media** has 0% MTA-STS adoption.

• **Education** leads DNSSEC at 34%, driven by university domains on .de ccTLD.

6. The Enforcement Gap

Of the 439 domains with a DMARC record, **156 (35.5%) remain at p=none**. This is the single most critical finding of this report.

A DMARC policy of p=none tells receiving mail servers to deliver emails that fail authentication anyway. The domain owner gets reports about spoofing attempts but takes no action to block them. Recipients remain unprotected.

Organizations typically get stuck in monitoring mode for three reasons: fear of breaking legitimate email from third-party services, lack of visibility into sending sources, and insufficient tooling to translate DMARC reports into actionable steps.

The following table shows enforcement rates by sector, sorted from worst to best:

Sector	DMARC Adoption	Enforcement	Gap
Education	87.7%	26.2%	61.5 pp
Telecommunications	92.3%	38.5%	53.8 pp
Government	77.1%	42.9%	34.3 pp
Media	92.1%	44.7%	47.4 pp
Healthcare	83.3%	56.2%	27.1 pp
Automotive	88.9%	61.1%	27.8 pp
Energy	86.4%	63.6%	22.7 pp
Insurance	90.9%	63.6%	27.3 pp
Banking	84.0%	64.0%	20.0 pp
Technology	87.9%	66.7%	21.2 pp
Transport	79.2%	66.7%	12.5 pp
Real Estate	100.0%	71.4%	28.6 pp
Industrials	90.6%	71.7%	18.9 pp
Chemicals	86.7%	73.3%	13.3 pp
Retail	100.0%	74.1%	25.9 pp
Consumer	95.7%	87.0%	8.7 pp

7. MTA-STS: The Forgotten Protocol

MTA-STS (Mail Transfer Agent Strict Transport Security) enforces TLS encryption for inbound email. Without it, an attacker can intercept SMTP connections and force emails to be transmitted in plaintext (a TLS downgrade attack).

Across the DACH region, **only 41 out of 503 domains (8.2%) have MTA-STS enabled**. This leaves 91.8% of analyzed domains vulnerable to email interception in transit.

Germany leads at 9.8%, while Austria (5.2%) and Switzerland (5.1%) trail behind. The chemicals sector has the highest adoption at 33.3%, while media has 0%.

Notable MTA-STS adopters include Allianz, BASF, Bosch, Commerzbank, Deutsche Bahn, E.ON, Fresenius, Henkel, Roche, SBB, and Vodafone DE.

8. DNSSEC Adoption

DNSSEC (Domain Name System Security Extensions) cryptographically signs DNS records to prevent cache poisoning and DNS hijacking attacks. **79 domains (15.7%) have DNSSEC enabled.**

Switzerland leads at 20.2%, followed by Germany (14.7%) and Austria (14.3%). The education sector has the highest adoption at 33.8%, driven by university domains benefiting from .de ccTLD DNSSEC signing.

9. Notable Findings

9.1 Major Organizations Without DMARC

64 domains (12.7%) have no DMARC record at all. Notable examples include:

Domain	Organization	Country	Industry
schaeffler.com	Schaeffler	DE	Automotive
bayernlb.de	BayernLB	DE	Banking
dz-bank.de	DZ Bank	DE	Banking
max-planck.de	Max-Planck-Gesellschaft	DE	Education
helmholtz.de	Helmholtz	DE	Education
ethz.ch	ETH Zürich	CH	Education
energie-ag.at	Energie AG	AT	Energy
koeln.de	Köln	DE	Government
nuernberg.de	Nürnberg	DE	Government
bremen.de	Bremen	DE	Government
dortmund.de	Dortmund	DE	Government
charité.de	Charité	DE	Healthcare
akh.or.at	AKH Wien	AT	Healthcare
kepleruniklinikum.at	Kepler Uni Klinikum	AT	Healthcare
carl-zeiss.com	Carl Zeiss	DE	Industrials
georg-fischer.com	Georg Fischer	CH	Industrials
swiss-life.ch	Swiss Life	CH	Insurance
faz.net	FAZ	DE	Media
delivery-hero.com	Delivery Hero	DE	Technology
fraport.com	Fraport	DE	Transport
dpd.com	DPD	DE	Transport

9.2 Major Organizations Stuck at p=none

The following well-known organizations have DMARC but remain in monitoring mode:

Domain	Organization	Country	Industry
volkswagen.de	Volkswagen	DE	Automotive
continental.com	Continental	DE	Automotive
sparkasse.de	Sparkasse	DE	Banking
fraunhofer.de	Fraunhofer	DE	Education
lmu.de	LMU München	DE	Education
kit.edu	KIT	DE	Education
univie.ac.at	Uni Wien	AT	Education
omv.com	OMV	AT	Energy
nrw.de	NRW	DE	Government

berlin.de	Berlin	DE	Government
baden-wuerttemberg.de	Baden-Württemberg	DE	Government
muenchen.de	München	DE	Government
bayer.com	Bayer	DE	Healthcare
rheinmetall.com	Rheinmetall	DE	Industrials
hannover-re.com	Hannover Rück	DE	Insurance
huk.de	HUK-Coburg	DE	Insurance
uniqa.at	UNIQA	AT	Insurance
bertelsmann.com	Bertelsmann	DE	Media
lidl.de	Lidl	DE	Retail
otto.de	Otto Group	DE	Retail
migros.ch	Migros	CH	Retail
zalando.de	Zalando	DE	Technology
flixbus.de	FlixBus	DE	Technology
swisscom.com	Swisscom	CH	Telecommunications
deutschebahn.com	Deutsche Bahn	DE	Transport
tuigroup.com	TUI	DE	Transport
oebb.at	ÖBB	AT	Transport

10. Recommendations

1. **Move beyond p=none.** If your domain has DMARC in monitoring mode, commit to a timeline for enforcement. Analyze your aggregate reports, identify all legitimate sending sources, fix SPF and DKIM for each one, and progress to p=quarantine then p=reject.

2. **Deploy MTA-STS.** At 8.2% adoption, MTA-STS is the most under-deployed email security protocol in the DACH region. It requires a DNS record and a policy file hosted over HTTPS. The setup is straightforward and protects against TLS downgrade attacks on inbound email.

3. **Enable DNSSEC.** With only 15.7% adoption, the majority of DACH domains remain vulnerable to DNS hijacking. Contact your DNS provider to enable DNSSEC signing.

4. **Prioritize government and education.** These sectors handle sensitive citizen and student data yet have the lowest enforcement rates. Regulatory pressure and institutional security policies should mandate DMARC enforcement.

5. **Automate monitoring.** DMARC is not a one-time setup. New sending sources are added, SPF records change, DKIM keys rotate. Continuous monitoring with actionable recommendations is essential to maintain enforcement over time.

---

11. About This Report

This report was published by **DMARCPulse** in April 2026. DMARCPulse is a DMARC monitoring platform that provides actionable recommendations for email authentication. The platform analyzes DMARC aggregate reports and generates specific DNS configuration suggestions for SPF, DKIM, MTA-STS, TLS-RPT, and BIMI.

The analysis covers 503 domains from public and private organizations in Germany, Austria, and Switzerland. Domain data was sourced from public stock indices, government directories, and institutional websites. All DNS queries used public resolvers.

This report is provided for informational purposes. The data reflects publicly observable DNS records at the time of collection. Organizations may have additional security measures in place that are not visible through DNS queries alone.

Contact

Web: https://dmarcpulse.io

Email: hello@dmarcpulse.io

LinkedIn: https://www.linkedin.com/showcase/dmarcpulse