POWERDMARC

EMAIL AUTHENTICATION INTELLIGENCE

Latin America DMARC & MTA-STS Adoption Report 2026

A sIX-market benchmark ot emall authentication entorcement - where the technical foundation is strong, but real protection is dangerously thin.

Brazil | Mexico | Ecuador | Argentina | Peru | Chie

108%
Yoy surge in cyberattacks (2025)

2,640
Avg weekly attacks per org

~99%
Business email without MTA-STS

#1 BR
Most-targeted LATAM market

Executive Summary

PowerDMARC analyzed email authentication across six major LATAM markets in this 2026 report: **Brazil, Mexico, Argentina, Ecuador, Peru, and Chile** (the latter based on a 2024 dataset). The results uncover a striking regional paradox: even though foundational technical setups are solid, actual security enforcement is dangerously lagging. In 2025, Latin America faced a **108% year-over-year surge in cyberattacks**, with organizations across the region now facing an average of 2,640 weekly attacks.

LATAM Cumulative Averages • 5-Market Comparable Cohort

93.1%	19.6%	0.9%	8.6%
SPF correctly configured	DMARC at p=reject	MTA-STS deployed	DNSSEC enabled
Strong foundation	Enforcement gap	Critical blind spot	Brazil carries the average

Key Takeaways

- **SPF adoption is high (70%–96%)** across all markets, proving solid foundational setup.
- **DMARC enforcement (p=reject) peaks at just 24.9% (Ecuador)** — most organizations fail to actually block spoofing attacks.
- **MTA-STS is virtually nonexistent** — roughly 99% of outbound business email is exposed to interception.
- **Media is the weakest sector** in every country analyzed, leaving public communication channels wide open to spoofing.
- **Ecuador leads LATAM in DMARC enforcement;** Brazil dominates DNS security via DNSSEC.
- **Peru records the lowest SPF adoption (86.1%)** and among the weakest enforcement rates in the region.
- **Chile's 2024 data shows the most severe baseline** in the cohort: 63.8% of domains with no DMARC record at all.

Why Is Email Security in Latin America Under Sustained Attack?

The fast pace of digital transformation across Latin America — fueled by explosive fintech growth, expanding e-government platforms, and cloud adoption — has expanded the digital attack surface much faster than defensive controls have evolved. Three structural vulnerabilities are shared across all analyzed markets:

01

The SPF-Enforcement Gap

Organizations configure foundational records but fail to implement strict DMARC policies — identifying themselves while leaving the door open for impersonation.

02

MTA-STS Blind Spot

Mail Transfer Agent Strict Transport Security is virtually nonexistent region-wide, leaving data vulnerable to interception and downgrade attacks.

03

Inconsistent Compliance

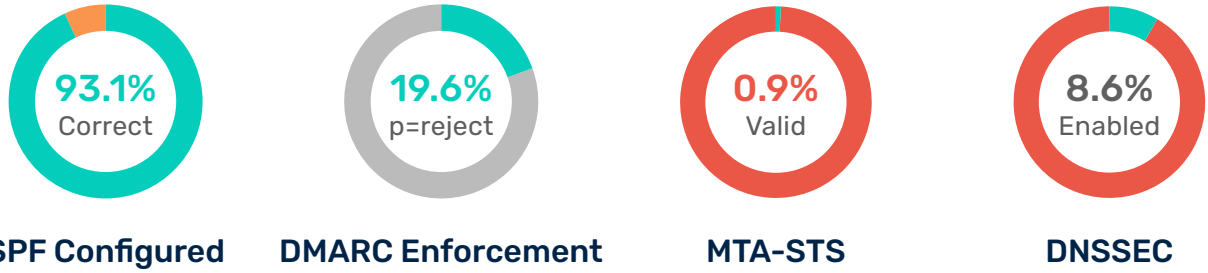
Enforcement is uneven across borders and industries, creating exploitable gaps in cross-border communication chains.

Email Security Across LATAM: The Big Picture

The cumulative view below ranks all six markets on the four pillars of email authentication. Chile is shown separately throughout, as its figures derive from a historical February 2024 dataset.

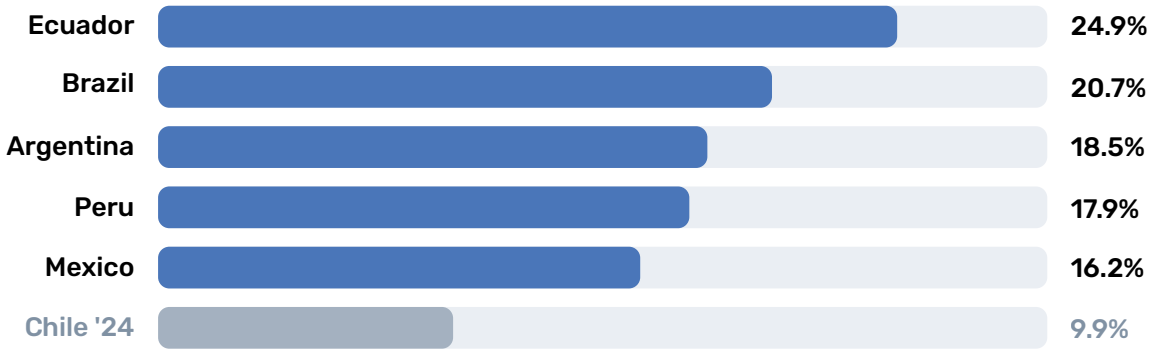
Regional Authentication Posture — LATAM Average

Share of domains across the six-market cohort meeting each control.



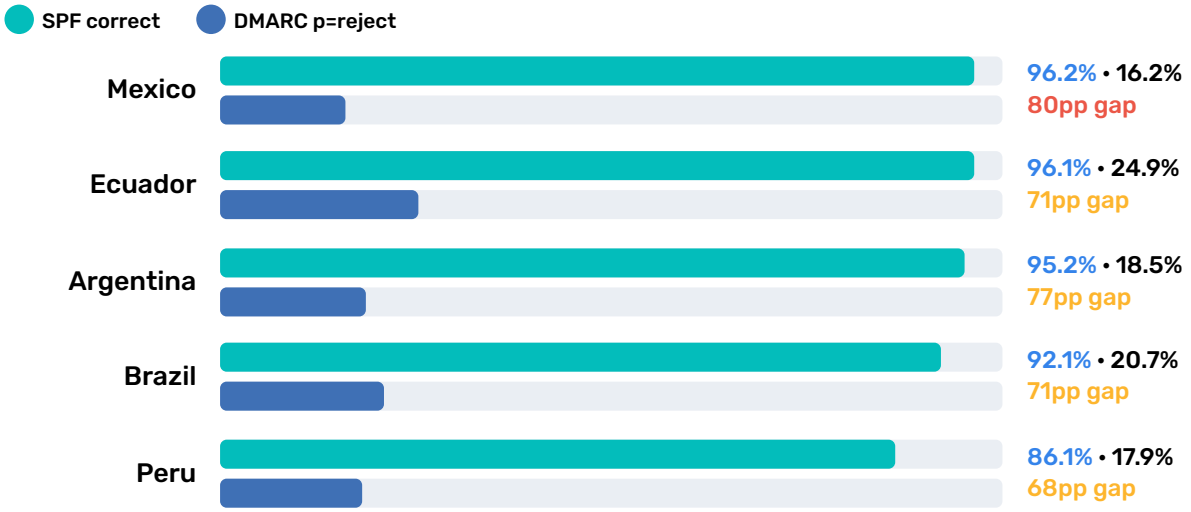
DMARC Enforcement Ranking — % of Domains at p=reject

Ecuador leads the region; no market clears 25%



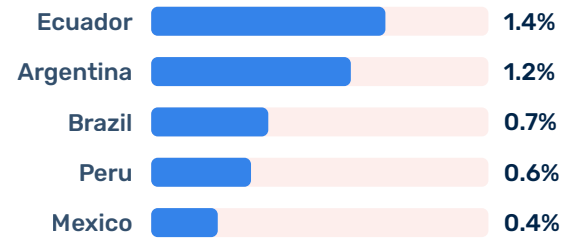
The SPF–Enforcement Paradox

A strong foundation (SPF, light) rarely translates into active protection (p=reject, dark). The gap is the exposure.



MTA-STS Adoption

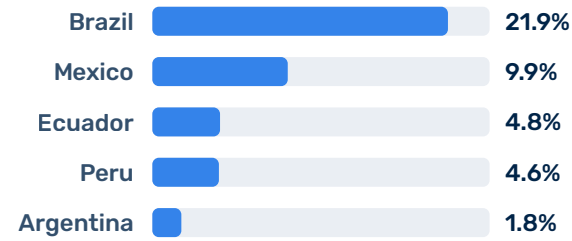
The regional blind spot — even the leader sits near zero



Axis 0–2% • ~99% of regional email is exposed

DNSSEC Adoption

Brazil is a regional outlier; the rest barely register



Axis 0–25%

6-Country Benchmark

Chile is evaluated separately due to its historical 2024 dataset.

Country	SPF Correct	p=reject	MTA-STS	DNSSEC	Standing
Ecuador	96.1%	24.9%	1.4%	4.8%	#1 • LATAM Leader
Brazil	92.1%	**20.7%**	0.7%	21.9%	#2 • DNSSEC Leader
Peru	86.1%	17.9%	0.6%	4.6%	#3 • Lowest SPF
Argentina	95.2%	18.5%	1.2%	1.8%	#4 • Lowest DNSSEC
Mexico	96.2%	16.2%	0.4%	9.9%	#5 • Lowest Enforcement
Chile (2024)	70.0%	9.9%	N/A	N/A	#6 • 2024 Baseline

Market-by-Market Deep Dive

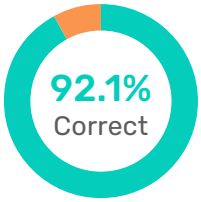
Each profile breaks the four authentication pillars into their full policy distribution, then drills into sector-level posture and risk.

Brazil

DNSSEC Leader • Media Crisis

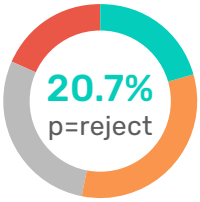
#2 LATAM

Latin America's most-targeted market enforces a strict p=reject policy on just **20.7%** of organizations. Its **21.9% DNSSEC** adoption leads the region — beating Poland (15.7%) and Japan (16.4%) — yet a 0.7% MTA-STS rate leaves nearly all email traffic open to transport interception.



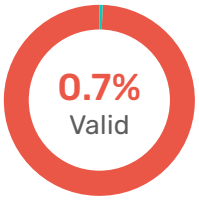
SPF

- correct 92.1%
- incorrect 7.9%



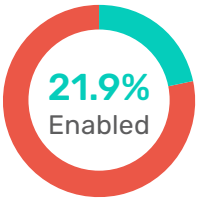
DMARC Policy

- p=reject 20.7%
- p=quarantine 32.5%
- p=none 28.5%
- No DMARC 18.3%



MTA-STS

- Valid 0.7%
- No MTA-STS 99.3%



DNSSEC

- Enabled 21.9%
- Disabled 78.1%

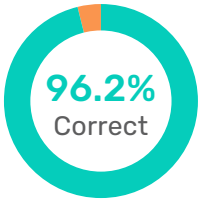
Sector	SPF	p=reject	MTA-STS	Risk
Finance	96.7%	39.2%	0%	Moderate
Government	97.8%	20.0%	0%	Moderate
Healthcare	90.0%	15.0%	0%	Critical
Education	93.0%	18.0%	0%	Moderate
Media	92.6%	6.4%	0%	Critical
Telecom	88.0%	22.0%	0%	Moderate

Mexico

Highest SPF • Lowest Enforcement

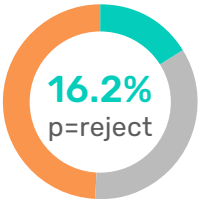
#5 LATAM

Mexico posts the region's highest SPF accuracy at **96.2%**, yet sinks to the bottom on enforcement at just **16.2%** p=reject. As many as 34.9% of domains remain stuck in monitoring (p=none) — despite a 74% ransomware hit rate and 43% perimeter-breach success rate during peak cycles.



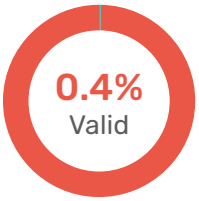
SPF

- correct **96.2%**
- incorrect **3.8%**



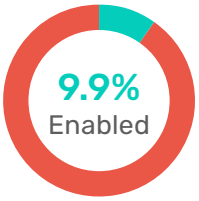
DMARC Policy

- p=reject **16.2%**
- p=none **34.9%**
- quarantine / no record **48.9%**



MTA-STS

- Valid **0.4%**
- No MTA-STS **99.6%**



DNSSEC

- Enabled **9.9%**
- Disabled **90.1%**

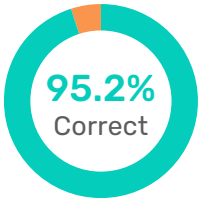
Sector	SPF	p=reject	MTA-STS	Risk
Finance	95.0%	29.1%	0%	Moderate
Government	97.0%	20.0%	0%	Moderate
Healthcare	90.0%	10.0%	0%	Critical
Education	94.0%	15.0%	0%	Critical
Media	93.0%	5.2%	0%	Critical
Transport	92.0%	9.5%	0%	Critical

Argentina

World-Class SPF • Critical Enforcement Gap

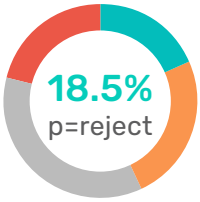
#4 LATAM

Argentina's **95.2% SPF** matches the United States, but protection falls off sharply — only **18.5%** enforce p=reject. A combined **56.9%** of domains remain fully exposed (35.9% at p=none, 21.0% with no record). CERT.ar logged 438 major incidents in 2024, 61% targeting government.



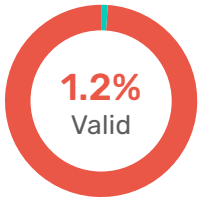
SPF

- correct **95.2%**
- incorrect **4.8%**



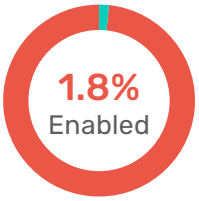
DMARC Policy

- p=reject **18.5%**
- p=quarantine **24.6%**
- p=none **35.9%**
- No DMARC **21%**



MTA-STS

- Valid **1.2%**
- No MTA-STS **98.8%**



DNSSEC

- Enabled **1.8%**
- Disabled **98.2%**

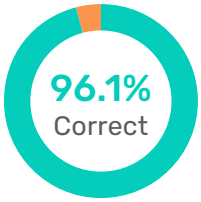
Sector	SPF	p=reject	MTA-STS	Risk
Banking	96.7%	28.4%	1.6%	Moderate
Healthcare	82.6%	8.7%	0%	Critical
Government	97.8%	26.1%	0%	Moderate
Energy	98.2%	28.6%	5.4%	Moderate
Media	92.6%	2.7%	0%	Critical
Transport	98.0%	30.6%	2.0%	Lower

Ecuador

LATAM's Enforcement Leader

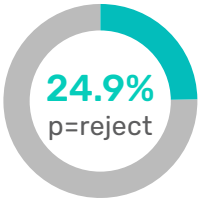
#1 LATAM

Ecuador takes the regional crown with a national enforcement rate of **24.9%** p=reject. Its financial sector hits **43.7%** — the highest single-sector enforcement metric recorded across the entire study. Healthcare, however, shows a stark inverse: just 4.4% enforcement with 47.8% lacking DMARC entirely.



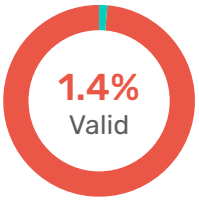
SPF

- correct **96.1%**
- incorrect **3.9%**



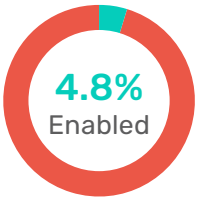
DMARC Policy

- p=reject **24.9%**
- Not enforcing **75.1%**



MTA-STS

- Valid **1.4%**
- No MTA-STS **98.6%**



DNSSEC

- Enabled **4.8%**
- Disabled **95.2%**

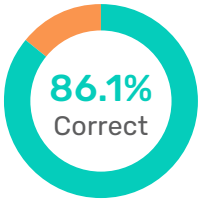
Sector	SPF	p=reject	MTA-STS	Risk
Finance	94.4%	43.7%	2.8%	Moderate
Healthcare	95.7%	4.4%	0%	Critical
Government	100%	14.3%	2.4%	Moderate
Energy	97.6%	34.1%	2.4%	Moderate
Media	100%	6.5%	0%	Critical
Transport	95.7%	34.8%	2.2%	Lower

Peru

Lowest Foundational Adoption

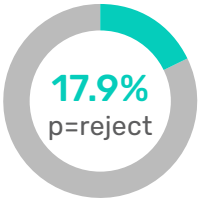
#3 LATAM

Peru sits in a tough spot foundationally with the region's lowest SPF adoption at **86.1%** — roughly 10 points behind Mexico and Ecuador. Its **17.9%** enforcement technically beats Mexico, but the underlying SPF gaps leave infrastructure highly vulnerable. Encryption matches the regional flatline: MTA-STS 0.6%, DNSSEC 4.6%.



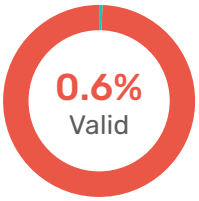
SPF

- correct **86.1%**
- incorrect **13.9%**



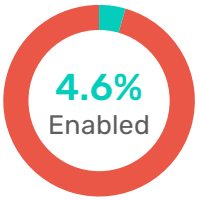
DMARC Policy

- p=reject **17.9%**
- Not enforcing **82.1%**



MTA-STS

- Valid **0.6%**
- No MTA-STS **99.4%**



DNSSEC

- Enabled **4.6%**
- Disabled **95.4%**

Sector	SPF	p=reject	MTA-STS	Risk
Healthcare	58.3%	20.8%	4.2%	Critical
Finance	84.4%	18.8%	0%	Critical
Government	94.3%	26.1%	0%	Moderate
Telecom	91.0%	9.0%	0%	Critical
Transport	80.0%	13.3%	0%	Critical
Education	84.7%	18.7%	1.7%	Moderate

Chile • 2024 Historical

Critical Baseline • Pre-Regulatory Reform

#6 • 2024

Methodology note: Chile reflects data captured February 2024 across 1,004 domains. It excludes MTA-STS / DNSSEC breakdowns and is not directly comparable to the 2026 benchmarks.

As of February 2024, Chile lagged significantly behind regional peers. **63.8%** of Chilean domains had no DMARC record whatsoever, and only **9.9%** enforced p=reject — the lowest baseline analyzed in Latin America.

SPF

correct	**70%**
incorrect	**30%**

DMARC Policy

p=reject	**9.9%**
Other policy	**26.3%**
No DMARC	**63.8%**

Sector	No DMARC Record	Note
Energy	77.4%	Worst-performing sector
Media	74.6%	Second-worst sector
Banking	51.0%	Prime financial targets largely unprotected

Four Patterns That Hold Across Borders

01 The SPF–Enforcement Paradox

SPF ranges 70–96%, but top enforcement is Ecuador's 24.9%. The reject gap is widest in Mexico (+80pp) and Peru (+68pp) — authentication is treated as one-and-done setup, not active protection.

02 MTA-STS is an Absolute Blind Spot

Single-digit adoption everywhere — Ecuador leads at just 1.4%. ~99% of outbound business email travels without enforced transport security, exposed to MitM and SMTP downgrade attacks.

03 Media is the Weakest Sector

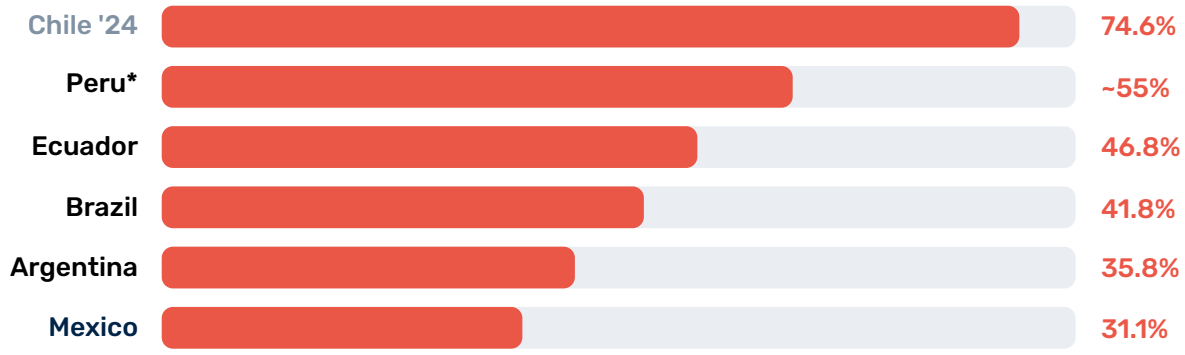
Across every market, Media & Entertainment is the weakest link — risking forged breaking-news alerts, stock manipulation, and disinformation through domain spoofing.

04 DNSSEC Highlights Brazil as an Outlier

Aside from Brazil's 21.9%, the region's DNS core is largely unprotected. Argentina's 1.8% — with 0% across Government and Education — leaves services exposed to cache poisoning.

Media Sector Exposure — % of Domains With No DMARC Record

The most vulnerable vertical in every market studied.



* Peru's report categorizes some vulnerable media domains under 'Miscellaneous'. Axis 0–80%.

Four Structural Weaknesses

1. The "Compliance Trap" of p=none

Across every market, organizations publish a basic DMARC footprint but stall at passive monitoring. Mexico leads at 34.9% stuck at p=none, Argentina at 35.9%. This provides oversight visibility but does nothing to stop an active forgery attack.

"Organizations frequently mistake visibility for safety. Real protection requires moving past monitoring and turning on automated defense at the security gateway."

Maitham Al Lawati, CEO, PowerDMARC

2. SPF Complexity & the 10-Lookup Limit

As LATAM networks deploy complex cloud ecosystems, SPF structures routinely break the 10-DNS-lookup limit, causing legitimate mail to fail and land in spam. Peru's healthcare (58.3% SPF correct) and Argentina's (82.6%) show this is a sector-wide crisis.

"Modern business networks quickly overload legacy SPF lookup limits. Applying automated SPF Flattening is essential to maintaining operational delivery and brand legitimacy."

Yunes Tarada, Service Delivery Manager, PowerDMARC

3. MTA-STS: The Encryption Blind Spot

With 99%+ of LATAM domains lacking MTA-STS, servers depend entirely on opportunistic encryption — open to downgrade attacks that strip traffic into readable plaintext. Ecuador leads at 1.4%; Peru and Mexico near-zero at 0.6% and 0.4%.

"Relying on opportunistic encryption creates a false sense of security. For LATAM operators, deploying managed encryption paths is critical to maintaining end-to-end payload confidentiality."

Ayan Bhuiya, Operations & Delivery Shift Lead, PowerDMARC

4. DNSSEC: The Foundation of Brand Trust

Outside Brazil (21.9%), DNSSEC adoption is critically low. Argentina's 1.8% means 98.2% of corporate identities remain exposed to cache manipulation and path hijacking; multiple countries record 0% in government and education.

"A DNS hijacking incident can instantly wipe out decades of customer trust. DNSSEC provides the cryptographic confirmation that your traffic goes to your authentic servers, not a criminal replica."

Ahona Rudra, Content Marketing Manager, PowerDMARC

What Should Organizations Do Now?

1 Audit Your Current Authentication Status

Verify your DMARC, SPF, and DKIM deployment with an automated tool like PowerDMARC's DMARC Record Checker. Know exactly where you stand before planning remediation.

2 Enforce Strict DMARC Policies

Over a third of domains in Mexico (34.9%) and Argentina (35.9%) sit at p=none. Move systematically from monitoring to quarantine to full p=reject.

3 Implement MTA-STS + TLS Reporting

Deploy MTA-STS alongside TLS Reporting to close the near-zero adoption gap exposing regional email to downgrade attacks — the most urgent unaddressed gap on the continent.

4 Prioritize Healthcare and Media Sectors

These verticals consistently display the highest risk in every country — Argentina's healthcare at 52.2% p=none, Brazil's media at 41.8% no-DMARC. Implement immediate mitigation controls.

5 Deploy Continuous Analytics

Use cloud-based analytics via PowerDMARC's DMARC Analyzer to monitor sending sources, track alignment, and surface spoofing attempts before they cause damage.

Appendix

Research Methodology & Data Sources

DNS Record Analysis

Active DNS queries across domain samples in each country, retrieving and validating SPF, DMARC, MTA-STS, and DNSSEC records per relevant RFC standards.

Sector Sampling

Domains identified from public national registries across Financial, Healthcare, Government, Education, Energy, Media, Telecom, and Transport. Chile data captured Feb 2024 (1,004 domains).

Global Benchmarking

Benchmark figures sourced from PowerDMARC's published country reports using a consistent DNS-analysis methodology.

Risk Classification

Sector risk ratings derived from a composite of p=reject adoption, share of domains with no DMARC record, SPF misconfiguration rate, and MTA-STS non-adoption.

Threat Intelligence

Regional threat data sourced from Kaspersky threat intelligence, CERT.ar incident logs, and regional cybersecurity industry reports covering 2024–2025.