DMARC REPORT

A Practical DMARC Guide for MSPs

Securing Client Email and Building a Scalable Managed Service

Table of Content

Email continues to be one of the easiest ways for attackers to reach businesses. Phishing, spoofing, and brand impersonation attacks rely heavily on email because it is trusted, widely used, and difficult to police without proper controls. For service providers responsible for protecting client environments, securing email identity has become a foundational requirement.

This is where DMARC plays a central role.

> DMARC (Domain-based Message Authentication, Reporting, and Conformance) helps organizations control how their domains are used in email. Instead of leaving inbox providers to guess whether a message is legitimate, DMARC gives clear instructions on how unauthenticated emails should be handled. When implemented correctly, it prevents attackers from sending email that falsely appears to come from a trusted domain.

For **Managed Service Providers**, DMARC represents more than a technical safeguard. It is a repeatable, high-value service that strengthens client security while creating an opportunity for long-term engagement.

This guide explains how DMARC works, why it matters specifically for MSPs, and how to deliver it as a managed offering. *It also outlines practical deployment steps, common pitfalls, and what to look for when choosing a DMARC platform built for multi-client environments.*

Understanding DMARC

DMARC is an **email authentication framework** that relies on SPF and DKIM to validate sending sources. Its purpose is to ensure that messages claiming to originate from a domain are genuinely authorized by that domain.

A DMARC policy is published in DNS and tells receiving mail systems how to treat messages that fail authentication. Domain owners can instruct inbox providers to:

- Take no action but send reports
- Route suspicious messages to spam
- Reject unauthenticated messages outright

In addition to enforcement, DMARC generates reporting data. These reports reveal which systems are sending email on behalf of a domain and whether those messages pass authentication checks. This visibility is critical for both security and deliverability.

Why Inbox Providers Expect DMARC

Email ecosystems have changed. Major mailbox providers now place greater emphasis on sender authentication, particularly for domains that send email at scale. **Marketing platforms**, transactional systems, and even routine business email are subject to increased scrutiny.

Domains without a properly configured DMARC policy are more likely to experience delivery issues such as spam filtering, throttling, or outright rejection. Weak or misaligned configurations can have the same effect.

For MSPs, this shift means clients increasingly depend on them to maintain email trust. DMARC is no longer a one-time DNS entry—it requires continuous oversight as sending sources evolve and infrastructure changes.

Why DMARC Is Important for MSPs

Managing DMARC across multiple customer domains delivers several benefits:

- Reduces the risk of phishing and spoofing attacks
- Stops threat actors from impersonating client brands
- Improves reliability of legitimate email delivery
- Protects brand reputation and **customer confidence**

> By enforcing DMARC, MSPs help ensure that only approved systems can send email using a client's domain. *This protects employees, partners, and customers from fraudulent messages while improving inbox placement for legitimate communication.*

Alignment, Visibility, and Reporting

DMARC relies on alignment between the domain in the "From" address and the domains used in SPF or DKIM. When alignment fails and a **strict policy** is applied, inbox providers can block or filter those messages automatically.

DMARC reporting adds another layer of value. Aggregate reports from mailbox providers reveal:

- Authorized and unauthorized sending sources
- Authentication failures caused by misconfiguration
- New services sending email without approval

For MSPs, this data enables proactive remediation rather than reactive cleanup after an incident.

Why MSPs Should Offer DMARC as a Managed Service

Many organizations recognize email threats but lack the expertise or time to manage authentication properly. This creates a clear opportunity for MSPs.

A Service Clients Understand

DMARC ties directly to outcomes clients care about: fewer phishing attacks, better email delivery, and stronger brand protection. It opens the door to broader security discussions without overwhelming non-technical stakeholders.

Ongoing Value, Not a One-Time Fix

Email environments change constantly. New **SaaS tools**, marketing platforms, and cloud services can break authentication overnight. DMARC requires ongoing monitoring and adjustment, making it ideal for a recurring managed service.

Reduced Risk for Clients

Enforced DMARC policies stop many impersonation attempts before they ever reach an inbox. This lowers exposure to fraud, credential theft, and business email compromise.

How MSPs Can Deploy DMARC Safely

Start With Monitoring

Begin with a policy that collects data without blocking messages. This phase builds visibility into all legitimate and unexpected senders.

Authenticate Approved Sources

Configure SPF and DKIM for every system that sends email on behalf of the domain. This step often requires coordination with third-party vendors.

Use the Right Tools

Manual DMARC management does not scale. *MSP-focused platforms allow teams to manage multiple domains, simplify reports, and reduce configuration errors.*

Monitor Continuously

New senders appear over time. Continuous monitoring ensures issues are caught early and corrected before they impact security or deliverability.

Enforce When Ready

Once authentication is stable, move to **quarantine or reject policies** to block impersonation attempts and strengthen trust with inbox providers.

Looking Beyond DMARC

While DMARC is essential, it does not address every domain-related threat. Attackers increasingly exploit unused subdomains, misconfigured DNS records, and lookalike domains to bypass email controls entirely.

A comprehensive approach requires visibility across the entire domain surface—not just email authentication.

DMARCReport extends protection by helping MSPs identify DNS risks, unmanaged subdomains, and configuration weaknesses that attackers can exploit. This allows service providers to deliver broader **domain-level security** without introducing unnecessary complexity.

Choosing the Right DMARC Platform for MSPs

When evaluating solutions, MSPs should prioritize:

- **Centralized management** for multiple clients
- Clear, actionable reporting for both technicians and customers
- Support for related standards like SPF, DKIM, BIMI, and TLS reporting
- Visibility into risks beyond basic DMARC enforcement

Why MSPs Choose DMARCReport

DMARCReport is designed specifically for service providers who manage email security at scale. The platform simplifies deployment, automates monitoring, and provides clear insights into every sending source across client domains.

With continuous visibility, alerting, and domain intelligence, **MSPs can detect issues early**, prevent abuse, and maintain healthy configurations as environments evolve. *Additional capabilities—such as DNS risk detection, brand abuse monitoring, and API access—enable MSPs to offer a more complete domain protection service.*

For MSPs looking to deliver dependable email security while building a scalable managed offering, DMARCReport provides the foundation to protect client domains and maintain long-term trust.

Free Tools

- DMARC Lookup Tool
- SPF Lookup Tool
- MTA-STS Lookup Tool
- BIMI Lookup Tool
- TLS-RPT Lookup Tool

DMARC REPORT

Contact Us


www.dmarcreport.com


support@dmarcreport.com


(+1) 855-700-1386

Reach Us on Social Media