SENDMARC

The DMARC Compliance Guide for MSPs & VARs:

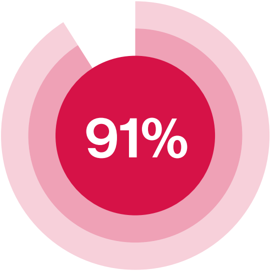
Grow your business, protect your clients

www.sendmarc.com

What's inside

Introduction

In today's threat-heavy digital landscape, email remains the top attack method for cybercriminals. 91% of all cybercrimes start with an email, with phishing attacks reaching an all-time high in 2023.



of all cybercrimes start with an email

Even after the 2023 peak, phishing attacks remained high through 2024, with almost 990 thousand attacks detected in the fourth quarter alone. From fake websites to spoofed messages, phishing and impersonation attacks are hitting millions of targets every year, affecting organizations of all sizes and industries across the globe.

As MSPs and VARs, you're on the frontlines of protecting your clients and their reputations from these threats.

This is where Domain-based Message Authentication, Reporting, and Conformance (DMARC) comes in. This global email authentication standard stops unauthorized use of your clients' domains to send fraudulent emails. It works with other authentication protocols Sender Policy Framework (SPF), and DomainKeys Identified Mail (DKIM), to shield them from phishing, spoofing, and impersonation attacks.

Today, DMARC has evolved from a best practice to a growing global requirement. Email providers, governments, regulators, and cyber insurers are calling for DMARC adoption, with compliance mandates increasing around the world.

DMARC implementation is also picking up pace globally as more businesses recognize the need for better email security and the key role the standard plays in compliance. The growing number of valid DMARC records in the DNS is clear proof of this trend. But nearly two-thirds of companies still rely on skilled MSPs or VARs like yours (with the help of a DMARC provider, like Sendmarc) to implement DMARC effectively and fine-tune its configuration. Ongoing support and continuous monitoring are also essential to maintain full compliance over time.

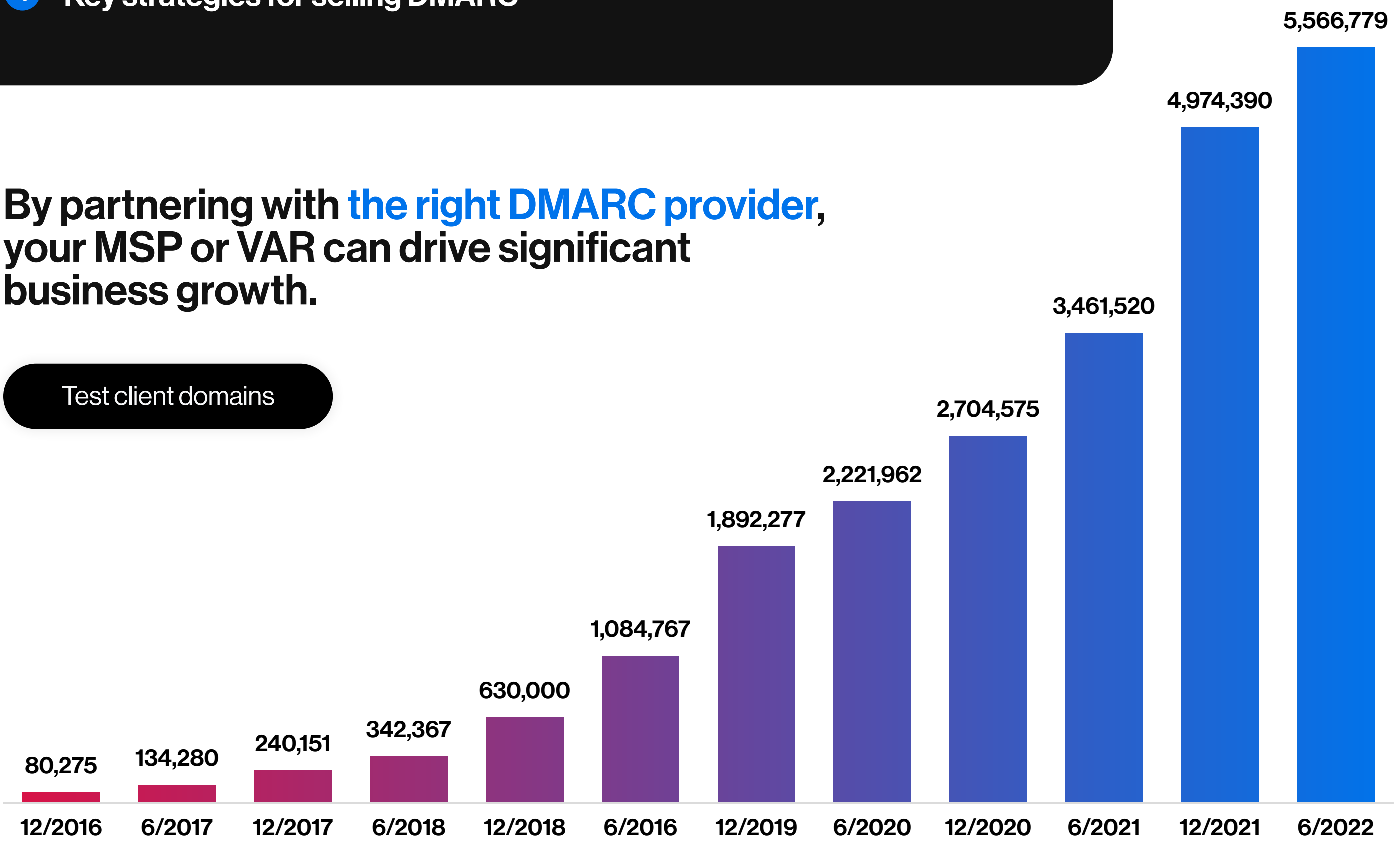
This presents a significant business opportunity for your MSP or VAR to leverage the DMARC compliance push to grow existing client relationships, create new leads, and provide a stronger cybersecurity offering.

In this guide, we'll explore:

1. Why DMARC is being mandated & becoming an industry standard
2. The DMARC compliance opportunity: Why MSPs & VARs should care
3. Compliance standards in more detail
4. Key strategies for selling DMARC

By partnering with the right DMARC provider, your MSP or VAR can drive significant business growth.

Test client domains



Valid DMARC records confirmed via DNS

Why the push for DMARC adoption?

For over a decade, organizations and regulatory bodies have recognized a need for DMARC. The recent surge in compliance mandates highlights the standard's key role in securing both senders and recipients from ever-increasing cyberthreats, while also strengthening the overall trust and integrity of digital communication.

The push for DMARC compliance led to a 60% increase in valid DMARC records in two months in 2024. While this is in part because of Google and Yahoo's requirements, it's also because adopting DMARC helps organizations improve compliance with requirements from regulators like the Payment Card Industry Data Security Standard (PCI DSS) v4.0, General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and more.

Microsoft join Google & Yahoo on mandating DMARC

In April 2025, Microsoft also announced that it would start requiring bulk senders - domains sending over 5 000 emails per day – to have SPF, DKIM, and DMARC in place by May 5. Non-compliant emails will be rejected.

> **While Microsoft's requirements apply to bulk senders, I believe every domain should have SPF, DKIM, and DMARC in place. These aren't just technical best practices - they're essential for protecting deliverability and reputation.**
>
> **Microsoft themselves say it best: 'All senders benefit from these practices.' It's time the industry starts moving in that direction.**

J. Peter Bruzzese

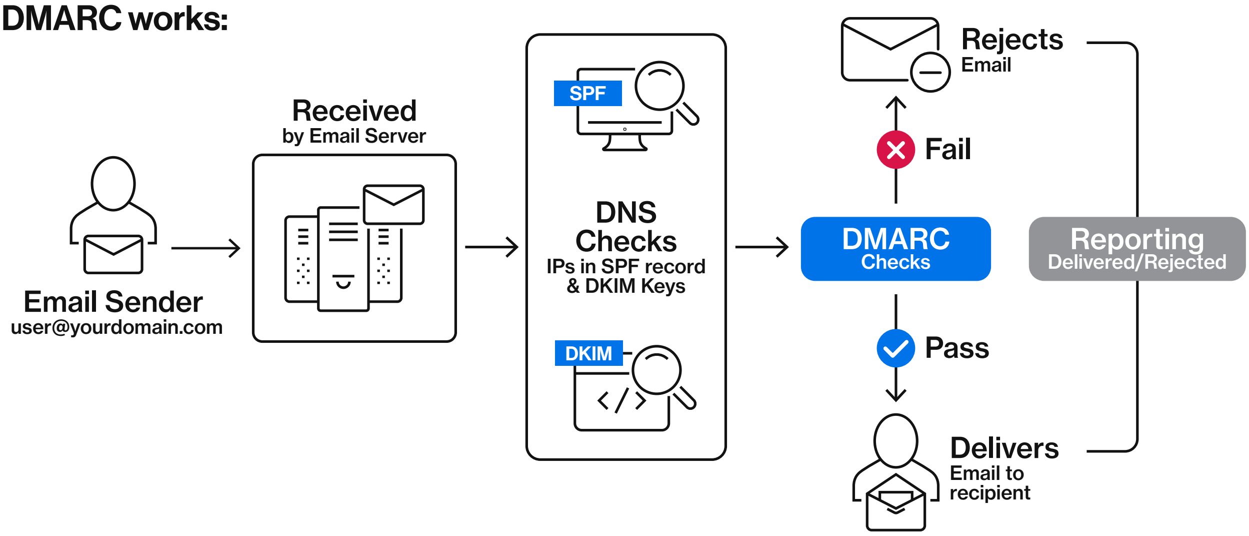
ClipTraining Co-Founder & Chief Content Officer
Host of Security Insights
Nine-time Awarded Microsoft MVP
Co-Founder of the Central Florida Microsoft 365 User Group

As cyberattacks continue to grow in numbers and sophistication, traditional email security tools, like anti-spam filters, employee training, or multi-factor authentication, are no longer enough to effectively secure your business or customers. These measures protect internal teams but do little to stop attackers from impersonating your clients' domains and targeting their customers, suppliers, or partners.

This is because a flaw in email's design means that it can't verify senders or block fraudulent messages, leaving the door open for domain spoofing. DMARC fills this gap, giving businesses the visibility and control they need to prevent cybercriminals from sending malicious emails using their domains.

Without this protection, your clients' businesses are left wide open to a range of email-based threats that can lead to serious operational, financial, and reputational consequences. It's this vulnerability that has led to the global push for DMARC adoption.

How DMARC works:



DMARC Benefits

Enhanced compliance is just one of DMARC's benefits for your clients; others include:

Increased security

DMARC verifies the sender's identity and message integrity and then decides what to do with an email, which helps reduce the chance that your clients fall victim to a phishing or spoofing attack.

Strengthened brand trust

With DMARC, companies can protect their brand from being used in fraudulent activities and show their commitment to protecting their customers, increasing trust and loyalty.

Boosted deliverability

Emails from domains that have a strong DMARC policy are more likely to reach the recipient's inbox instead of the Junk or Spam folder, enhancing communication.

Improved visibility & control

It provides organizations with reports on who's sending emails on their behalf, allowing them to identify and authorize legitimate senders and block malicious ones.

A real-world example of cyberattack damage

Sector: Insurance

Business size: 800+ employees

Business challenge: An insurance company had a complex email environment, and customers were receiving fraudulent emails posing as them, marketing emails were ending up in Spam folders, and their email deliverability performance was lacking.

After DMARC implementation:

Increased email deliverability

Email deliverability was significantly improved by implementing a strong DMARC policy

Enhanced email security

The support team received fewer email abuse cases

Improved visibility

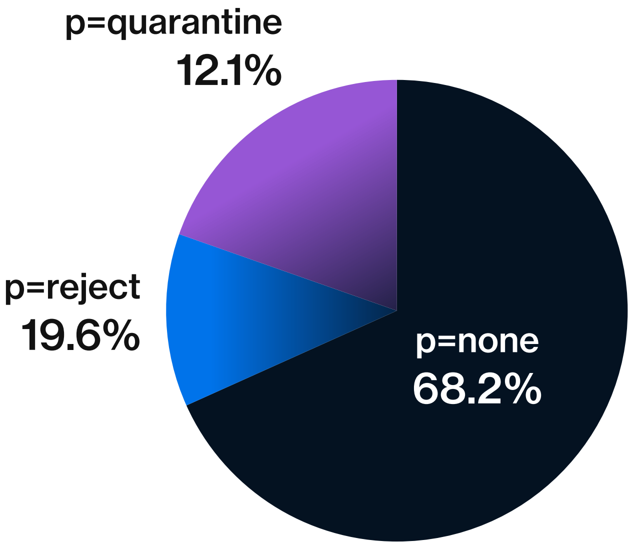
Their visibility on attacking source patterns increased, allowing them to leverage data into other systems

The DMARC compliance opportunity: Why your MSP or VAR should care

While global mandates and recommendations for DMARC have increased its adoption, most domain owners have implemented it with a policy of p=none. This could be because the DMARC rules from email giants like Google, Yahoo, and Microsoft, which have contributed to adoption in a big way, only require a policy of none for compliance right now.

But it's also because businesses are concerned that implementing stricter policies will affect the deliverability of their legitimate emails. While a p=none DMARC policy is a good starting point to monitor email traffic, it doesn't provide any protection for your clients.

This has created a need for you as an IT provider to drive the adoption of stronger DMARC policies within your customer environments, promoting both protection and compliance.



These statistics come from a specific dataset that examines only domains that use DMARC and doesn't cover all email domains globally. This dataset's trends are believed to represent internet-wide trends and so provide valuable insight.

So, what's the opportunity?

With DMARC compliance becoming a must, businesses everywhere are feeling the pressure, but most don't have the in-house skills to get it right. The technical expertise needed to implement DMARC effectively means that MSPs and VARs specializing in DMARC are in high demand. This puts you in a great position to take the lead and deliver real value where it's needed most.

- ✓ 2/3 Companies **need help setting up DMARC** effectively
- ✓ Join the **growing DMARC market** expected to be worth $1.72B by 2028
- ✓ Fulfil a need for **approximately 70%** of your customers

(Sources: Sendmarc market research, Digital Journal)

The role DMARC plays in compliance

While DMARC isn't required by all regulations, **its ability to verify email authenticity helps organizations meet multiple compliance standards**. As previously mentioned, DMARC is also an essential layer of defense in the current digital landscape. It protects your business's and clients' emails by verifying the sender, safeguarding against phishing and spoofing.

Understanding compliance standards

While implementing DMARC helps senders meet rules from email giants like Google, Yahoo, and Microsoft, it also improves overall compliance with regulatory standards. To show its value, we've provided details on how DMARC aligns with a few well-known mandates and regulatory requirements.

Standard	Requirements	How DMARC helps
Payment Card Industry Data Security Standard **(PCI DSS)** v4.0	Requires businesses to implement anti-phishing mechanisms to protect cardholder data.	DMARC verifies email sources and reduces organizations' risk of phishing attacks for both internal and external stakeholders.
California Consumer Privacy Act **(CCPA)**	Enforces customer data protection.	DMARC helps secure sensitive information contained within emails.
National Institute of Standards and Technology Cybersecurity Framework **(NIST CSF)**	Organizations are required to reduce cybersecurity risks through proactive email security	DMARC helps identify and prevent email-based threats, detect suspicious activity, and respond quickly to protect domains.
General Data Protection Regulation **(GDPR)**	Protect personal data and privacy in the EU.	DMARC secures email communications to reduce the risk of data breaches.

Below are some of the organizations that promote DMARC as a standard. To view more click here.

Government Digital Service

European Commission GDPR General Data Protection Regulation

gfma GLOBAL FINANCIAL MARKETS ASSOCIATION

computer emergency response team CERT-EU for the EU institutions, bodies and agencies

FINRA

PCI Security Standards Council

IETF

Microsoft

yahoo!

Gmail

Selling DMARC: Key steps to success

Using the information from this guide, you can follow this 4-step process to start conversations with your clients:

1 Show clients their vulnerability

Using analysis and reporting tools, like Sendmarc has, you can show customers exactly who is sending emails from their domains and where these senders are in the world. This often reveals unknown or unauthorized sources, making the risk feel real.

2 Highlight the threats & potential damages

Explain that email phishing, spoofing, and impersonation are growing threats that could lead to damages like deposit fraud, identity theft, and potentially irreparable reputational damage. Implementing DMARC protects business revenue streams by reducing cyberattack risks and securing their hard-earned good reputation.

3 Talk about compliance

Briefly walk clients through how DMARC will help them meet global mandates and recommendations from email platforms, governments, and regulators in their region. Position your MSP or VAR as the expert partner who makes DMARC compliance simple, helping your clients avoid penalties, protect their reputation, and meet regulatory demands.

4 Highlight DMARC's benefits

From protecting brand reputation and finances to improving deliverability, DMARC has many benefits. Make it clear that DMARC not only enhances compliance and security, but also builds brand trust, visibility, and gets their emails into the inbox.

Discovery questions for value-based conversations

A key component of value-based conversations is mastering the art of discovery. We've put together a list of discovery questions to **help you uncover what truly matters** to your client or potential client:

1. Do you currently have a **way to monitor which services send emails** on your behalf, both authorized and unauthorized?

2. What email security **measures do you have in place** to prevent impersonation and interception?

3. Have you ever had **issues with email spoofing or phishing attempts** that appeared to come from your domain?

4. Have you **experienced any significant email security incidents** in the last year?

5. How do you think a **security breach or fraudulent payments** involving your email domain would affect your company's reputation?

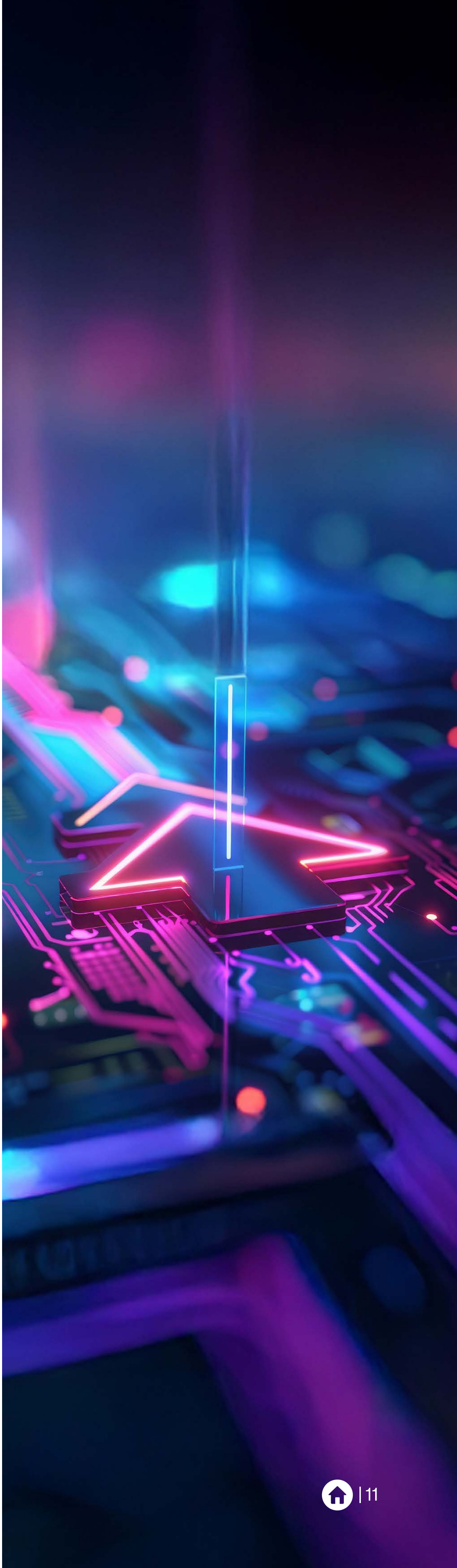
6. What would you say the impact would be in **ensuring 100% of your marketing emails** make it to your prospective customers' inboxes?

7. What impact would faster, **more secure email processes** have on your team's productivity?

8. We can provide **real-time reporting, alerts, and ongoing monitoring.** How important is that level of insight to you?

9. Customers using our DMARC service have seen a **significant increase in customer trust**, increased engagement, and higher conversion rates. How do you think this would affect your customer relationships?

10. What metrics would you use to **evaluate the success** of a DMARC implementation?



Manual vs. Automated DMARC
Which is better?

DIYing DMARC is risky as it can cause issues that often result in unintentionally blocked legitimate emails. The need for ongoing management and adjustments also requires technical expertise and time. **Let's compare the requirements and outcomes of each:**

Manual		Automated with Sendmarc
12+ Months Manual setup & implementation require extensive time & effort	Time to enforcement & protection	**Less than 90 days*** The Sendmarc team gets your domain DMARC compliant & protected as fast as possible
Unreliable Incorrect configuration & misidentification of sending sources could lead to unintentionally blocked legitimate emails or delivery of fraudulent email	Chances of successful implementation	**Guaranteed** Every legitimate sender is correctly configured & DMARC compliant, maximizing email delivery
Manual & time-consuming Reports from various email service providers are delivered as raw XML files, requiring decoding	DMARC reporting	**Automated** Reporting data in a summarized & explained format, in one place, on the Sendmarc platform
High-effort Resources dedicated to sender identification & configuration with potential of lost revenue due to interrupted email flows. Dedicated resource needed to monitor & manage	Implementation effort	**Effortless** Implement & manage DMARC on Sendmarc's user-friendly platform with expert support as needed

*For customers on Sendmarc's Premium Plan.

Grow your business with Sendmarc

Sendmarc's Partner-first approach to DMARC implementation

The right people

A team of committed global DMARC experts who care and are passionate about collaborating to create a safer Internet for everyone.

A unique promise

The only DMARC company that guarantees clients full protection within 90 days.*

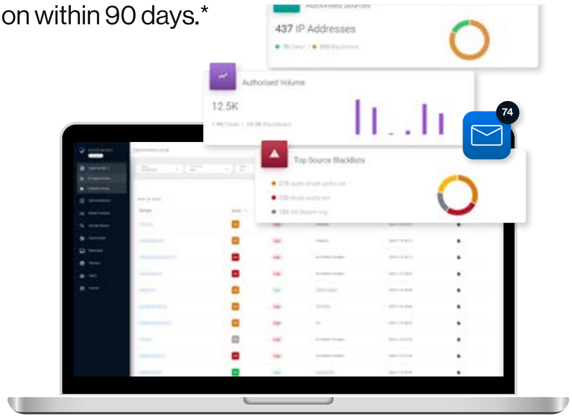
*For customers on Sendmarc's Premium Plan.

Simple pricing

Easy to quote, effortless for clients, and scales to any budget with pricing models tailored to suit any business size.

Our Onboarding & Learning Academy

Become a Sendmarc expert with tools to fast-track your DMARC skills and knowledge.



A partner-first platform

Our leading DMARC platform is built to accelerate your success by supporting your sales and protection needs through a user-friendly interface and full feature set.

Customer Portal

- **Co-branded platform** seamlessly integrates our services into your product bouquet
- **Multi-tenant solution** empowers efficient & simplified control of your client base
- **Automated DNS updates** improve efficiency by enabling fast adjustments
- **Alerts & integrations** enable live monitoring
- **Task management** for managing & guiding implementations across your client base
- **Full API** to enable custom integrations & reporting
- **Integration into PSA platforms**

Partner Portal

- **Website domain testing widget** increases lead generation
- **Opportunity analysis tools** highlight vulnerable customer domains to easily identify sales opportunities
- **Marketing & sales enablement tools** to help you maximize the Sendmarc opportunity
- **Domain history reports** for simplified change tracking
- **Demonstration tool** to show existing & potential customers what impersonation could look like for their businesses

Ready to build a profitable business with DMARC?

Book a demo