DMARCsimple – DMARC Overview

DMARCsimple – DMARC Overview (Executive Summary)

What is DMARC?

DMARC (Domain-based Message Authentication, Reporting & Conformance) is an email authentication standard that helps domain owners protect their brand and recipients from phishing, spoofing and impersonation attacks. It works alongside SPF and DKIM to verify that email really came from your organization.

Without DMARC, attackers can send messages that appear to come from your domain and most recipients cannot easily tell the difference. With DMARC in place, mailbox providers gain clear instructions on how to treat messages that fail authentication.

Why DMARC matters

• Reduce phishing and spoofing by making it harder for attackers to impersonate your domain.

• Improve deliverability by demonstrating that you authenticate and monitor your email.

• Build trust with customers, partners and regulators.

• Gain visibility into who is actually sending on your behalf, including third parties and legacy systems.

How DMARC works

When a receiving mail server gets a message from your domain, it checks SPF and DKIM to see whether the message is authorized and aligned. DMARC then tells the receiver what to do if those checks fail. Common policies include:

• p=none – Monitor only. Mail is delivered, but reports show what would have been blocked.

• p=quarantine – Suspicious messages can be treated as spam or placed in a junk folder.

• p=reject – Messages that fail DMARC can be rejected outright, preventing spoofing.

Where DMARCsimple fits

DMARCsimple is designed to make DMARC approachable for real-world teams. Instead of sifting through raw XML reports, you get dashboards, trends and practical guidance that bridge the gap between business, marketing and IT. Visual dashboards show pass/fail and sending sources, and practical suggestions help fix SPF, DKIM and alignment issues safely.