DMARCsimple – Security & Compliance Summary

DMARCsimple – Security & Compliance Summary

DMARCsimple focuses on one critical attack surface: email identity. By helping you authenticate messages and monitor domain usage, DMARCsimple reduces the risk of phishing, spoofing and brand impersonation—issues that often appear in risk registers, audit findings and incident reports.

SOC 2 Alignment

• Logical access and change management – DMARC records and policy changes can be documented and reviewed as part of your configuration management process.

• System monitoring – Ongoing DMARC report ingestion and review represents a form of continuous monitoring over email identity.

• Risk mitigation – DMARC adoption reduces the likelihood and impact of email-based impersonation incidents.

ISO 27001 Alignment

• A.5 – Information security policies: Email authentication can be included as a formal requirement in your policies.

• A.12 – Operations security: DMARC reporting and monitoring can be treated as an operational control.

• A.13 – Communications security: Protects an essential communication channel against spoofing and fraudulent use.

HIPAA and Regulated Industries

• Helps limit PHI-related phishing attacks that impersonate trusted domains.

• Supports administrative and technical safeguards by strengthening email workflows.

• Provides audit-friendly evidence that email identity is actively monitored.

PCI DSS and Financial Services

DMARCsimple helps demonstrate that you are addressing email-based fraud and social engineering risks that can impact cardholder data environments and customer trust.

Platform Security Posture

DMARCsimple is built and maintained by a security-focused hosting and development team. While details may vary by deployment, goals include hardened hosting environments, encrypted transport, segmentation of tenant data, controlled access and ongoing monitoring and improvement of the platform.