brigantia

Email Security

SENDMARC

Stop email impersonation, and ensure your brand can be trusted with DMARC

Email is a prime target for cyber threats, constituting over 91% of network attacks. Cybercriminals are adept at exploiting unprotected email domains, posing as trusted sources. Without protection, they can convincingly impersonate brands and employees, making it challenging for MSPs and their customers to detect fraudulent activities. Potential consequences include deposit fraud, ransomware attacks, identity theft, and reputational damage. Sendmarc addresses this vulnerability through the implementation of DMARC.

DMARC serves as a crucial security measure by verifying the origin of an email and determining its legitimacy. Achieving DMARC compliance provides MSPs and their customers complete visibility and control over all emails originating from a domain. This standard validates the authenticity of the sender, ensuring that only legitimate emails are delivered. If an email fails the authentication process, it is promptly rejected.

Enhance the trustworthiness of the most widely used communication tool for your customers.

Benefits for MSPs and Their Customers:

Enhanced Visibility of Email Sources:
DMARC reporting allows MSPs to monitor both legitimate and illegitimate use of email domains. Achieving full protection status ensures the rejection of all unauthorised emails, providing continuous monitoring and management of the entire email ecosystem.

Trusted Email for the Entire Stakeholder Community:
MSPs can ensure that all inbound and outbound emails are verified for authenticity, thwarting cybercriminals from exploiting the customer's name for illicit gain. This guarantees that employees, customers, partners, and suppliers only receive legitimate emails.

Global and Company-Wide Compliance:
Apply globally recognised technical authentication and verification standards to all emails using the customer's brand name. This ensures compliance with every email service used across various departments.

Improved Email Deliverability:
Implement the strongest authentication rules and policies, guaranteeing that all legitimate emails under the customer's name reach their intended inboxes.

Strengthened Brand Recognition & Trust:
MSPs can help customers implement BIMI, an email authentication standard that displays the customer's logo next to emails in the recipient's inbox. This enhances brand recognition, trust, and ensures effective email communication by boosting deliverability.

Zero Infrastructure Costs - Provided as a Service:
Delivered through a purpose-built platform, MSPs can offer DMARC compliance without incurring infrastructure costs. The deployment is simplified with fully automated processes, real-time reporting access, and continuous proactive management of the entire email environment.

Guaranteed Security for Every Customer:
Deploy the same product with identical features and functionality for every customer, ensuring a consistent level of security. All customers receive the same 90-day guarantee to reach full protection.

Protection for the Entire Email Ecosystem:
Seamlessly integrate and implement DMARC with all third-party providers of email services, ensuring the security and safeguarding of the entire email real-estate.

Deliver DMARC compliance to your customers with Sendmarc Purpose-Built Platform:
The purpose-built platform ensures swift implementation of DMARC compliance for customers, providing interoperability to assess and manage data from multiple email service providers.

Rich Features for All:
The product is designed with a rich set of features and functionality, offering every customer the same level of protection. There are no gradings, tiers, or variations, as every organisation, regardless of size, is vulnerable to the same cyber threats and requires consistent standards of protection.

Contact Brigantia

Suite 2.1, Hurstwood Business Centre, York Road, Thirsk, YO7 3BX

Tel: 020 3358 0090 | Email: partnersupport@brigantia.com | Web: www.brigantia.com