DMARC Assure

SPOCHUB®
SaaS PaaS On Click

DMARC ASSURE

PRODUCT BROCHURE

OVERVIEW

Countless emails are sent daily. However, you are not the only valid user sending emails from your domain!

Your Web servers, CRM Applications, Volume mail gateways, External Marketing Agencies, Application Servers also send Emails to Customers/ Stakeholders/ External users using your Domain.

DO YOU KNOW??

SPOCHUB®
SaaS PaaS On Click

ANYONE CAN IMPERSONATE YOUR DOMAIN & SEND EMAILS USING YOUR LOOK-ALIKE DOMAIN TO YOUR CUSTOMERS / STAKEHOLDERS?

Over 82% of Business enterprises worldwide fall prey to domain spoofing/ impersonation crimes by Cyber Criminals. This leads to enormous irrevocable financial loss jeopardizing the Brand's reputation.

Primarily, SPF & DKIM were the two independent Email Authentication technologies that were used as security measures to prevent domain spoofing.

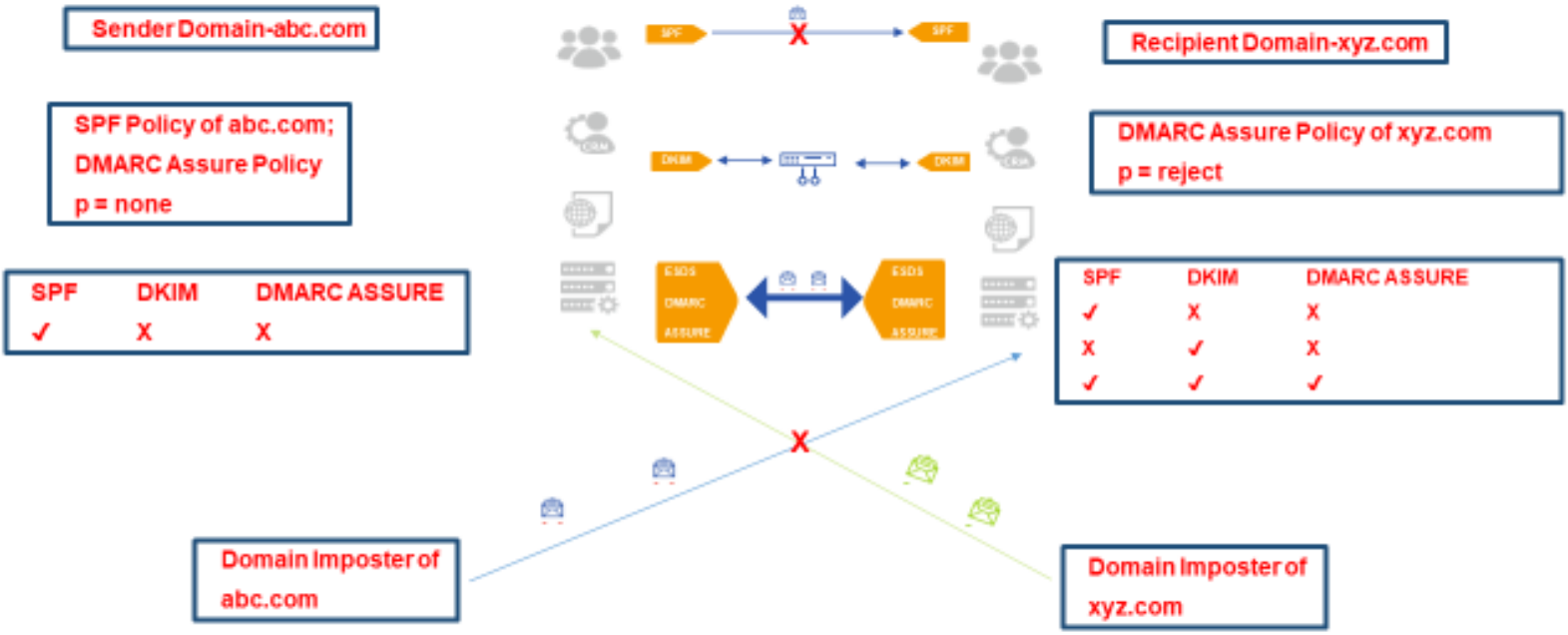
SPF -

Sender Policy Framework or SPF gives domain owners control over which IP addresses or hostnames can send emails on their behalf. SPF authentication is done on the Return-Path or the Envelope-Sender address, which is not visible to the Recipient.
Flip side- SPF fails to validate forwarded emails as the forwarder's SPF does not contain the original Sender's authorized IP address.

DKIM -

DomainKeys Identified Mail or DKIM validates the Sender using public key (asymmetric) cryptography, specifically RSA digital signatures. The record contains a DKIM version and the public key. DKIM assures that the email content has not been modified in-transit. Every Incoming email gets verified for DKIM records, while for outgoing Email DKIM is being stamped for each email.

HOW DO EMAIL GATEWAYS AUTHENTICATE OR TREAT AN EMAIL ARRIVING FROM A SENDER DOMAIN BEFORE DELIVERING IT TO THE RECIPIENT?

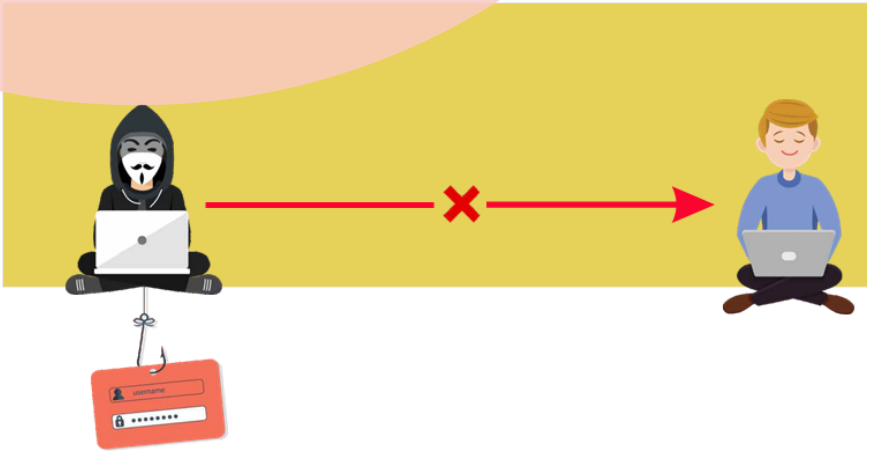


HOW DO EMAIL GATEWAYS AUTHENTICATE OR TREAT AN EMAIL ARRIVING FROM A SENDER DOMAIN BEFORE DELIVERING IT TO THE RECIPIENT?

- It falls under the prerogative of the recipient domains to check the Email Authentication measures of the sender domain & act as per their set policies. When an email lands at the Recipient domain's gateway, the recipient domains checks for SPF, DKIM & DMARC ASSURE authentication measures being adopted by the Sender domain. Every domain owner must announce to the Email Gateways worldwide as to how to treat & validate/authenticate emails coming from their domains.

- Consider a sender domain abc.com that only implies SPF as email authentication for their incoming & outgoing mail traffic. The recipient domain xyz.com has implied SPF, DKIM & has also announced a DMARC ASSURE decision policy matrix to all Email Gateways, set as p=Reject.

HOW DO EMAIL GATEWAYS AUTHENTICATE OR TREAT AN EMAIL ARRIVING FROM A SENDER DOMAIN BEFORE DELIVERING IT TO THE RECIPIENT?



When a mail is sent from abc.com to xyz.com, the DNS server of xyz.com, which is the Recipient domain checks whether the Sender domain has set any DMARC ASSURE policies. Finding only SPF as the email authentication measure, the email is delivered to the recipient user of xyz.com. The worst fear is when an imposter with malicious intent will spoof abc.com's domain name & send emails to Customers, Partners & Stakeholders on their behalf. Those will also get delivered as abc.com as it is not armed to tackle domain spoofing & phishing.

For abc.com to be able to prevent the misuse of their domains, it needs to adopt DKIM & DMARC ASSURE. Initially, abc.com's DMARC ASSURE policy will be set as p=NONE till the time they are sure to comply with strict SPF & DKIM policies, bringing their outgoing mail servers under the compliance. When the DMARC ASSURE policy is set as p=Quarantine, those emails will not be rejected outright; they will be delivered in the SPAM folder tagged as [Quarantine]. Once the compliance level reaches up to 90%, then they can confidently announce their DMARC ASSURE policies to be p=Reject to all Recipient Email Gateways. Cybercriminals will not be able to spoof their Domain & send an illegitimate email, maligning their brand name.

While users from abc.com are well protected by SPF, DKIM & DMARC ASSURE policy set as p=Reject, even if an imposter who has spoofed the Domain of xyz.com tries to send an Email to abc.com users, the mail will get rejected. DMARC ASSURE provides instructions to Email gateways to block messages that fail SPF and/or DKIM authentication verification and have a DMARC ASSURE record policy set to reject (p=reject).

DMARC ASSURE

IS A POWERFUL SECURITY MEASURE THAT HELPS BUSINESS ENTERPRISES TO:

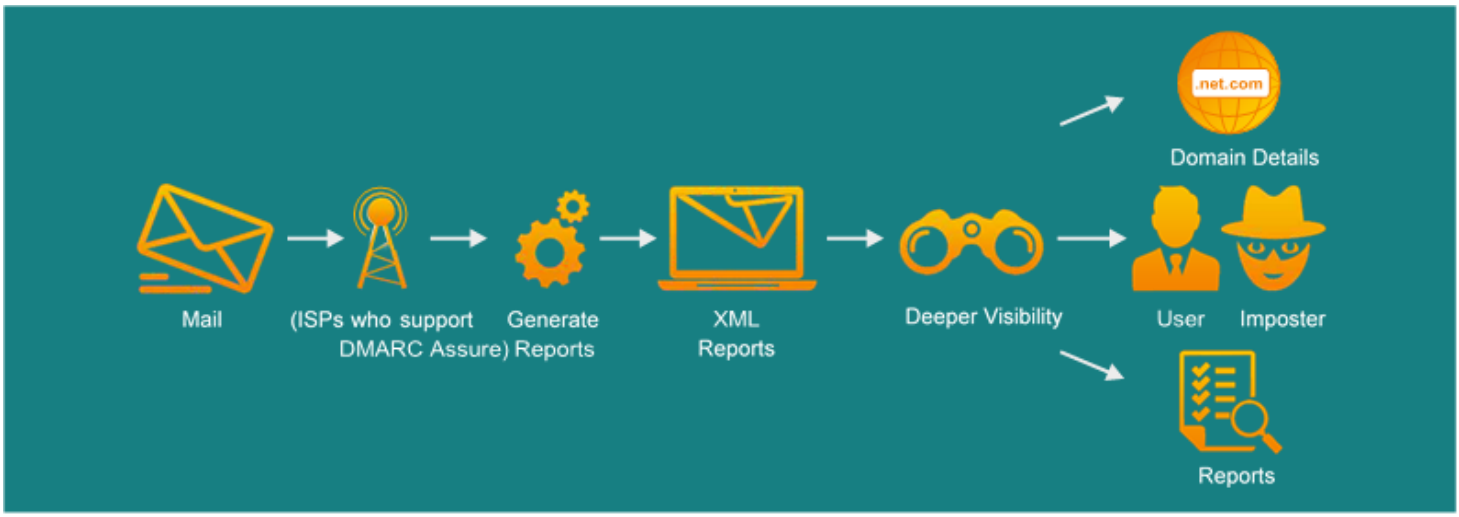
Obtain complete clarity and control over all your email channels

Authenticate and improve the deliverability of your emails

Block inbound attacks and safeguard your brand name

Publish an efficient policy that instructs ISP's to deliver or delete emails

HOW DMARC ASSURE WORKS??



1.Publish its email authentication practices.

2. State what actions should be taken on mail that fails authentication checks.

3. Enable reporting of these actions taken on mail claiming to be from its Domain.

4. ISPs who support DMARC ASSURE generate reports on the sending activity for your Domain.

5. The reports are XML files that are emailed to the email address specified in your DMARC ASSURE record.

6. The reports contain the sending source (domain/IP) along with whether the message passed or failed SPF and DKIM. Not only does it allow you to control email security for your Domain, but it also gives you deep visibility into who is sending on your behalf AND if they are signing with DKIM or passing SPF.

DMARC ASSURE

MAKE YOUR DOMAIN A "NO PHISHING ZONE"

Our team will handhold you through a well-defined action plan to achieve maximum compliance for your organization.

After implementing DMARC ASSURE, Organizations will begin to receive raw data with many potential insights into their email traffic. ESDS has core expertise in interpreting these reports & define action plans to achieve maximum compliance. The reports that DMARC ASSURE Monitor generates can help identify:

Servers/IP's which are sending email on behalf of your domains. These servers/IP's can be identified and SPF appropriately updated. All servers, including the corporate email system, will have to pass through a common email gateway, which enforces DKIM.

DMARC ASSURE also enables senders to receive data back from receivers, providing insight into fraudulent email patterns. There are only three DMARC ASSURE policies that a sender can specify, and thus, three deployable configurations for DMARC ASSURE

DMARC ASSURE

SPOCHUB®
SaaS PaaS On Click

MAKE YOUR DOMAIN A "NO PHISHING ZONE"

p=none:
Tells the receiver to do nothing to the message except report back to the Sender that it failed DMARC ASSURE validation. The Sender tells the receiver to deliver the message but lets the Sender know why it failed DMARC ASSURE validation.

p=quarantine:
Tells the receiver to treat the message as spam, results in delivery of the message to the recipients' junk/ spam folder, and then tells the receiver to report back on why the message failed validation.

p=reject:
Tells the receiver to block the message and report back on why the message failed validation.

The Above steps ensure that all legitimate mails are following compliance, till we reach more than 90 % Compliance, DMARC ASSURE should be configured as p=quarantine, If constantly DMARC ASSURE shows above 90 %, the same can be set as p=reject

KEY FEATURES

Tailor-made DMARC Services	**DMARC Assure helps you mitigate risks and block malicious emails working like an expert guide and helping business enterprises put an efficient reject policy into place.**
Simplified Deployment	**Our DMARC deployment and project management specialists are always ready to assist you in selecting our DMARC Assure services: viz: 1. Basic compliance checks and reports. 2. Advisory services to ensure compliance and effective anti-phishing.**
User-friendly Dashboard	**We offer various overviews of your DMARC data, which you can filter based on a specific date range. In the overviews, we give tips on which hosts are not yet fully optimized. You can directly link to the third-party documentation about this subject in that specific tool.**
Detailed Phishing Messages	**Our tool offers forensic reports from DMARC. This ensures you can track invalid email flows faster. This overview is grouped based on a detailed message.**
Assess	**The reports that DMARC Assure generates can help identify servers / IP's which are sending email On- Behalf of your domains & works on Implementing DMARC Policies after assessing the status.**

KEY FEATURES

Reports, Analysis & Interpretations

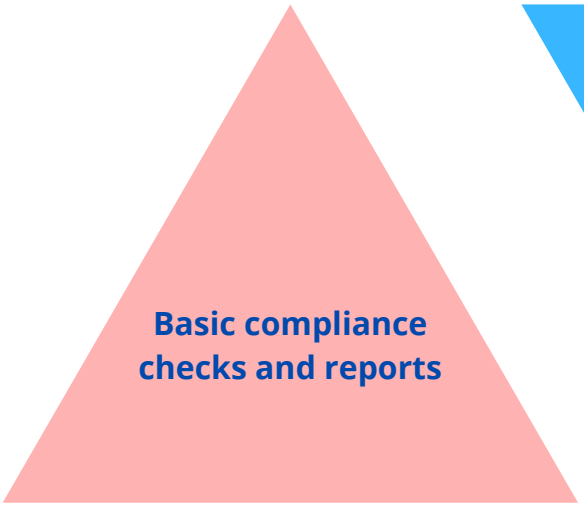
Daily or Weekly reports are sent on request. These reports show the DMARC compatibility rate for all your domains. ISPs supporting DMARC generate XML Reports that are sent to the Email address specified in your DMARC Record, providing deep visibility into who is sending Emails on your behalf and if they are signing with DKIM or passing SPF. The reporting and data received after implementing DMARC can be difficult to interpret. Fortunately, if senders are willing to invest, this can be solved with managed services, who can take the data and turn it into actionable insights for senders.

Cloud Domain Spoofing

Cousin domain or look-alike spoofing instance is currently on a rampage. Alarmingly, they tend to surpass Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), as well as Domain-Based Message Authentication, Reporting and Conformance (DMARC) check.
Cousin domains typically are used as a phishing tool to spoof your Brand's domain name. For instance, amit@E5DS.in (it is the numeric 5, instead of the alphabet S) is a cousin domain of amit@ESDS.co.in
Our team at ESDS has added Cousin Domain Spoofing as an additional security feature to identify such cousin domain spoofing instances when the domain name can be easily misspelled to make it look like the authorized/original Domain.

OUR SERVICES

SPOCHUB
SaaS PaaS On Click



We assist customers with their DMARC Implementation &
Our DMARC ASSURE analyzes DMARC Reports so as to start the journey of DMARC p=none to p=quarantine
Finally, Destination of p=reject