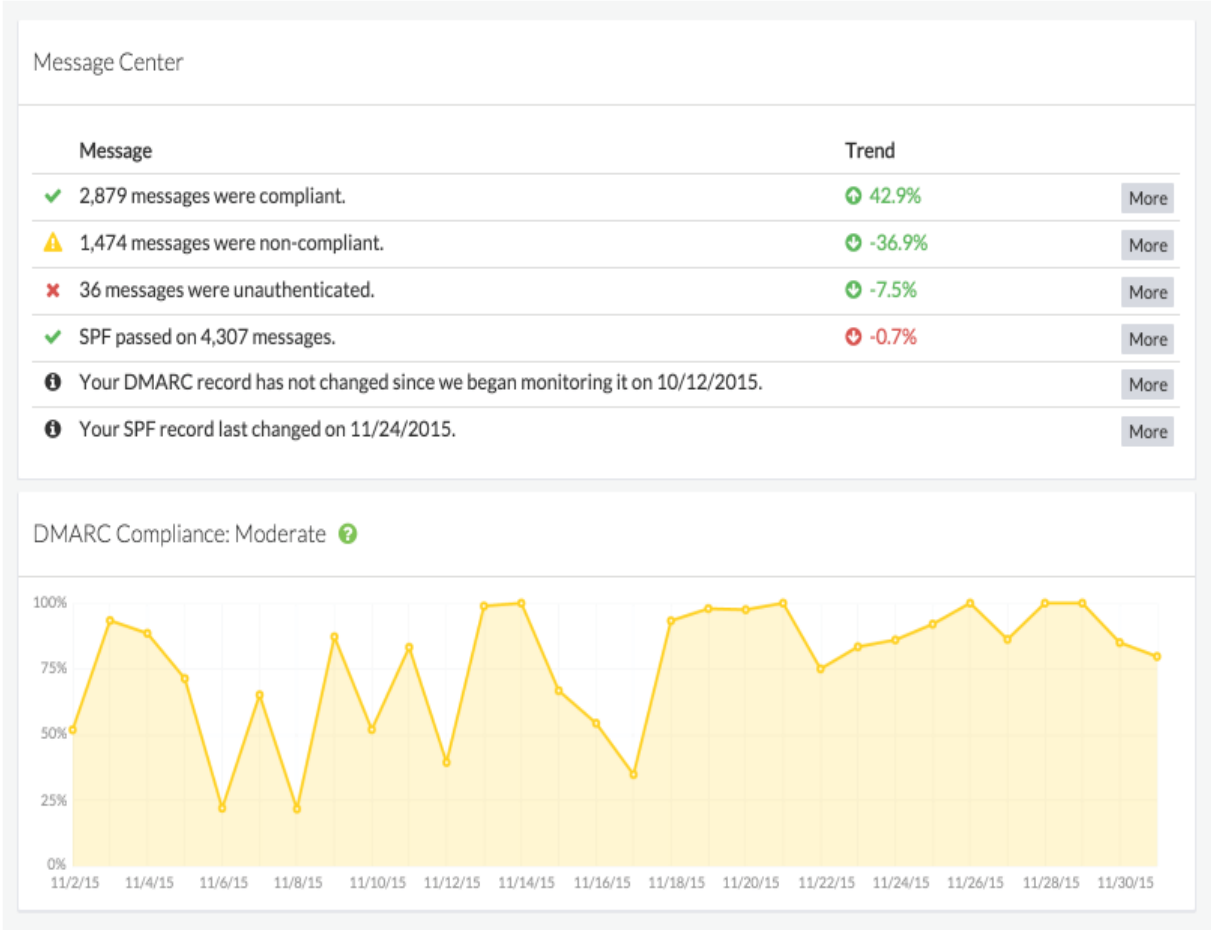
Deter fraudulent activity with

DMARC DASHBOARD

DMARC adoption is on the rise.

Worldwide, over 80% of consumer accounts are protected by DMARC. ASR Team's DMARC Dashboard is designed to guide you through implementing your own policy with ease. You can now join companies like PayPal, Twitter, Facebook, Gmail, Hotmail, Yahoo, and others in protecting your users by deterring fraudulent mailing activity.



ASR Team, LLC
30 Newbury Street Suite 3
Boston, MA 02169
www.asrteam.com

Report, analyze, and protect.

Going from observation to protection (via a "quarantine" or "reject" policy) is the ultimate goal. Without ASR Team, you'd have to make the transition with very little insight into the process, and that can be confusing. With ASR, you have a team of experts helping you take every step down the path to compliance and protection:

Report (Observation)

During observation, ASR will collect and analyze your DMARC reports to bring authentication issues to your attention and help you improve your compliance

Protect (Reject)

The final step is protecting your reputation by instructing receiving mailboxes to reject all inbound messages that fail DMARC authentication.

Analyze (Quarantine)

During quarantine, ISPs will treat compliance failures as suspicious. ASR then analyzes reports to help you identify false positives and fraudulent mail sources.

Deter fraudulent activity with

DMARC DASHBOARD

Intelligent Guidance

Utilizing DMARC's "observation mode," we analyze compliance and suggest corrective action, ultimately guiding you towards a quarantine or reject policy.

Message Center

The message center is designed to alleviate the confusion around deploying DMARC by summarizing compliance and authentication results.

Threat Map

The threat map provides a visual time lapse of threat sources around the world to give you visibility into unverified mail sources.

Compliance Scoring

Once we're receiving your DMARC reports, we'll score ("Good," "Moderate," etc.) your DMARC performance to set a clear benchmark for improvement.

Forensics Explorer

Forensic reports provide a detailed view of messages that failed against your DMARC policy and include samples and headers for investigation.

Multi-Domain

Our platform supports DMARC deployment across any number of domains to track compliance with mail streams of any size.

Questions?

support@asrteam.com