Enterprise Strategy Group | Getting to the bigger truth.™

ESG SHOWCASE

Overcoming the Challenges Associated with Achieving DMARC Enforcement

Date: January 2022 **Author:** Dave Gruber, Principal ESG Analyst

ABSTRACT: The prolific use of email impersonation and spoofing techniques has escalated the importance of DMARC email security controls; however, IT and security teams continue to struggle to achieve full DMARC enforcement. While SPF, DKIM, and DMARC provide the foundational mechanisms to combat email impersonation, the implementation process for DMARC projects can be long and manually intensive, causing many to abort them before realizing value.

New automated, self-service solutions are helping organizations overcome DMARC implementation challenges, speeding projects and helping organizations achieve full DMARC enforcement. This paper explores the DMARC opportunity, its implementation process and the challenges associated with it, and an innovative approach to successful DMARC enforcement. New strategies are needed.

Executive Summary

Impersonation and spoofing attacks are a significant issue for most organizations, growing at a much faster rate than standard malware attacks as cyber-criminals exploit human weaknesses. Attackers are targeting organizations and employees, together with their customers and suppliers, cultivating risk of damage to their brand, business relationships, and the successful delivery of outbound business email communications.

Differentiating between legitimate and fraudulent senders is key to defend against phishing, motivating many to fund Domain-based Message Authentication, Reporting, and Conformance (DMARC) enforcement initiatives to prevent domain-spoofed emails from being delivered. Government regulations are also making it mandatory for many to implement enforced DMARC to improve the security of their email communication channel.

When implemented with full enforcement, DMARC offers an effective, proven approach to stop spoofing and misuse of domains, protecting organizations against brand abuse and scams that can tarnish their reputations and disrupt organizational objectives directly, or indirectly through customers and partners. Yet while many have attempted DMARC implementation projects, IT and security teams often struggle during the implementation process, causing them to stop short of achieving DMARC enforcement. ESG research reports that, while 50% of organizations were using DMARC, only 26% of them made it to full enforcement.[1]

New approaches are needed to simplify, guide, and assist organizations in their DMARC implementations. This paper explores the DMARC opportunity, highlighting the challenges associated with the implementation process, together with the introduction of an innovative approach to achieve successful DMARC enforcement.

[1] Source: ESG Research Report, *Trends in Email Security*, August 2020.

This ESG Showcase was commissioned by Island and is distributed under license from ESG.

Combatting Impersonation with DMARC

DMARC can effectively defeat email impersonation when used in conjunction with a broader defensive arsenal. DMARC builds on existing SPF and DKIM email authentication techniques by adding a critical element: reporting.

However, many large organizations struggle to effectively implement these mechanisms to defend against this ongoing threat, continuing to leave them vulnerable to attack.

The Basics about SPF, DKIM, and DMARC

To protect against domain spoofing, three standard mechanisms have been created that result in the creation and management of a domain validation strategy: SPF, DKIM, and DMARC.

Sender Policy Framework

In simple terms, the Sender Policy Framework (SPF) is an email authentication protocol that can be leveraged to detect and stop spammers and attackers from successfully sending messages that *appear* to come from a trusted domain. SPF enables organizations to publish a list of authorized email sender servers through the DNS infrastructure using an SPF record. Receiving mail servers can then verify inbound emails by querying SPF records to verify if the IP address from which the email is sent matches an IP address in the domain's SPF record.

DomainKeys Identified Mail

DKIM, or DomainKeys Identified Mail, is an email authentication method that uses a digital signature to let the receiver of an email know that the message was sent and authorized by the owner of a specific domain. Once the receiver determines that an email is signed with a valid DKIM signature, it can be confirmed that the email's content has not been modified. In most cases, DKIM signatures are not visible to end-users, as the validation is done on a server level.

DMARC

DMARC, or Domain Message-based Authentication, Reporting, and Conformance, adds the final, important component of the solution, enabling email receiving servers to report and govern what domains (and associated sending IP addresses) are allowed to enter through inbound email. By leveraging the DNS infrastructure to share sender policy with email receiving servers, DMARC policy specifies what to do when emails fail DMARC authentication checks, instructing email receivers on how non-compliant messages should be handled—monitor and deliver (p=none), move to the junk folder (p=quarantine), or reject (p=reject).

Executive Involvement First

Successful DMARC projects often start with senior management involvement, including both CIO and CISO. This ensures both visibility to the approach and commitment to the resources required for a successful project.

The DMARC Implementation Process

Having an enforced DMARC policy enables an outbound layered protection against malicious actors sending email on behalf of an organization’s domains. When a malicious actor sends an email attempting to spoof a domain, the receiver will reject messages that fail the DMARC check and never deliver those messages to the inbox.

Successful DMARC projects often start with senior management involvement, including both CIO and CISO. This ensures both visibility to the approach and commitment to the resources required for a successful project.

The leadup to DMARC enforcement requires an organization to do a fair amount of prework, including:

1. Creating an inventory of the domains it needs to protect.
2. Inventorying all authorized email senders who are allowed to generate and send emails on its behalf.
3. Ensuring every authorized sender is set up to support both DKIM and DMARC.

This process can take anywhere from one to twelve months or more and requires an ongoing commitment to review and analyze significant amounts of DMARC reports sent by email receivers over this time.

DMARC Implementation Challenges

While DMARC is a proven, effective defense against domain impersonation, achieving enterprise DMARC enforcement can be a complex and time-consuming process, causing many to abort projects before successful completion, especially if they have many active and dormant domains or use multiple third parties to send email on their behalf.

According to the Mimecast *State of Email Security* report SEOS 2021,[2] less than a third of respondents are successfully using the DMARC email authentication protocol to stop bad actors from delivering harmful emails that appear to come from their brand's domain. This statistic is driven by the complexity of the process required to achieve full DMARC enforcement. Let's take a closer look at each of the three major steps in the process and highlight the challenges.

Step 1: Domain Inventory

While IT and security teams are aware of *most* domains in use by their organization, there are often unknown domains still in use. Unknown domains happen for a variety of reasons, including older/cancelled past projects, shadow-IT projects, and merger and acquisition (M&A) activities, making domain inventory a challenge for many larger organizations.

Centralizing Domain Management

Implementing a centralized process can both build a current domain inventory and keep it up to date in support of ongoing DMARC enforcement.

Most organizations lack a centralized domain management process, so implementing a centralized process can both build a current domain inventory and keep it up to date in support of ongoing DMARC implementations. The key to successful processes includes notifying all organizations to involve the domain management team when engaging with any external vendor who may communicate through email.

Step 2: Vendor (email sender) Inventory

Inventorying all vendors that send email on behalf of each domain has similar challenges to creating the domain inventory, including unknown shadow-IT projects and M&A activities. DMARC itself can help with the discovery of unknown senders. When a DMARC DNS record is set to monitoring mode, email receivers are instructed to send DMARC reports back to the domain owner, helping with unknown sender discovery. This process also highlights malicious senders.

DMARC reporting can generate overwhelming amounts of reports and require significant time reviewing the data to validate which domains are valid and which are invalid or spoofed. This process can go on for months, requiring continued investment of resources. Over time, confidence will build with the domain/vendor inventory. However, this is the step where many organizations bail out of the process due to the amount of time and effort required.

[2] Source: Mimecast State of Email Security Report, April 2021.

Step 3: DMARC Enforcement

Once the DMARC implementation team gains confidence in their vendor and email sender inventories, enforcement can begin. DMARC controls are opt-in controls, meaning that only approved-sender emails will be accepted; all others will be rejected.

For those confident in their inventories, SPF DNS records can be added or updated to include the full list of valid senders. However, when IT and security teams have doubts about the completeness of sender inventories, many choose to stop short of enforcement due to a fear of potential disruption to some portion of business operations based on DMARC rejected emails.

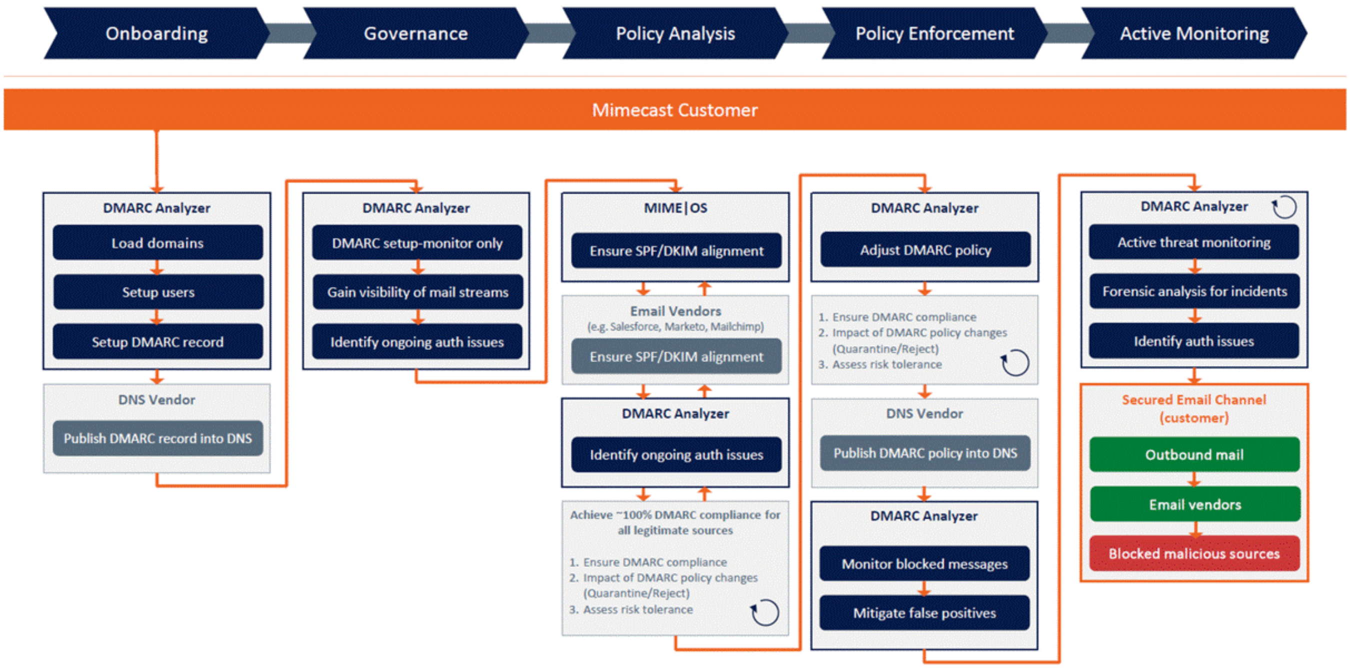
Each vendor/sender needs to also be contacted to verify that they are prepared to implement DMARC enforcement, including DKIM implementation. Larger SaaS vendors, such as Salesforce.com, ServiceNow, Marketo, Klaviyo, and others are already prepared, but special attention may be required for smaller-scale senders. Once notified, DMARC DNS records can be updated for each domain and typically set to isolation, quarantining any unknown sender for review.

Overcoming DMARC Challenges - Introducing Mimecast DMARC Analyzer

Mimecast DMARC Analyzer helps IT and security teams deploy DMARC in a user-friendly and frictionless way, providing a path to both ease and speed the process of moving into policy enforcement (p=reject), even in the most complex environments. The self-service solution provides the reporting and analytics needed to gain full visibility and governance across all email channels in use, reducing the time and resources required to become successfully DMARC compliant, while stopping the abuse of "owned domains" by cyber-criminals as part of phishing and spam attacks.

Mimecast DMARC Analyzer is delivered as a 100% software-as-a-service (SaaS) solution for rapid deployment and cost effectiveness.

Figure 1. Mimecast DMARC Analyzer – Deployment Workflow Step-by-Step


Onboarding
Governance
Policy Analysis
Policy Enforcement
Active Monitoring
Mimecast Customer
DMARC Analyzer
Load domains
Setup users
Setup DMARC record
DNS Vendor
Publish DMARC record into DNS
DMARC Analyzer
DMARC setup-monitor only
Gain visibility of mail streams
Identify ongoing auth issues
MIME|OS
Ensure SPF/DKIM alignment
Email Vendors
(e.g. Salesforce, Marketo, Mailchimp)
Ensure SPF/DKIM alignment
DMARC Analyzer
Identify ongoing auth issues
Achieve ~100% DMARC compliance for all legitimate sources
1. Ensure DMARC compliance
2. Impact of DMARC policy changes (Quarantine/Reject)
3. Assess risk tolerance
DMARC Analyzer
Adjust DMARC policy
1. Ensure DMARC compliance
2. Impact of DMARC policy changes (Quarantine/Reject)
3. Assess risk tolerance
DNS Vendor
Publish DMARC policy into DNS
DMARC Analyzer
Monitor blocked messages
Mitigate false positives
DMARC Analyzer
Active threat monitoring
Forensic analysis for incidents
Identify auth issues
Secured Email Channel (customer)
Outbound mail
Email vendors
Blocked malicious sources

Source: Mimecast

Mimecast DMARC Analyzer Managed Service

The Mimecast DMARC Analyzer Managed Service provides customers with end-to-end DMARC implementation, enforcement, and monitoring support. Delivered by experts in the field, the Managed Service delivers proactive guidance to set up a DMARC record and then move from monitor (with a DMARC "none" policy) to quarantine and, ultimately, 100% reject. Once full reject has been accomplished, the specialists will assure email channel governance. The customer will work closely with the Managed Service specialists to troubleshoot authentication failure issues, minimize the risk of inadvertently blocking legitimate emails, and benefit more quickly by blocking spoofed and phishing emails. In the event of an email phishing or security incident, Mimecast can assist with message-level details and forensic investigation to provide the incident response team with information on the source and size of attacks and share insights on other indicators of compromise.

The Bigger Truth

With impersonation involved in most successful cyber-attacks, security teams *must* confront this escalating attack technique. DMARC is a viable, proven approach to curb domain impersonation. Achieving full DMARC enforcement has its challenges. However, with the support of assistive solutions such as Mimecast DMARC Analyzer, full DMARC enforcement can be achieved with existing IT and security teams. ESG recommends organizations, including those that have attempted and failed to reach DMARC enforcement in the past, explore solutions from vendors like Mimecast to understand how they facilitate successful DMARC implementations.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com ✉ contact@esg-global.com ☎ 508.482.0188