

FORTRΔ™

Getting Started with DMARC

Secure your email.

Stop phishing.

Protect your brand.





Table of Contents

The History of Email Authentication	3	Putting DMARC Into Practice	9
Introduction to the Basics		The Big Picture	
What Is DMARC?	4	It's Worth a Thousand Words	10
The Benefits of DMARC		The Results of Implementing DMARC	
Why You Should Care	5	A Real World Example	11
The Bonus to Implementation		The Numbers Today	
DMARC and Inbound Threats	6	DMARC Adoption Worldwide	12
The Standards		The Challenge to Implementing DMARC	
A Closer Look At SPF, DKIM, and DMARC	7	What Makes DMARC Implementation Hard	13
The Mechanics		The Decision	
How DMARC Works	8	Selecting the Right Vendor	14
The Process			



The History of Email Authentication

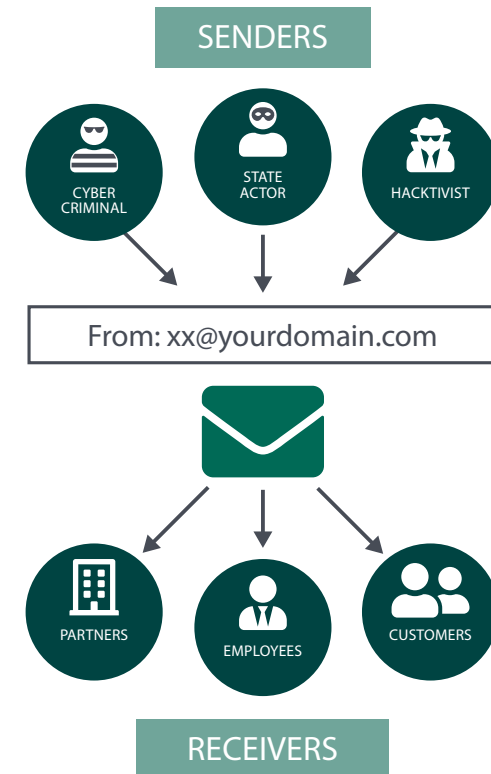
Email—despite its importance, ubiquity, and staying power—has never been secure.

Prior attempts at security have failed to solve email’s fundamental flaw—anyone can send email using someone else’s identity. This flaw has put the power of the world’s most admired brands in the hands of cybercriminals. Through email, criminals can use almost any brand or email domain to send spam, phishing emails, and malware installs, inflicting direct losses to customers and eroding the brand equity companies have spent years building.

Many of the most respected brands in the world, including Facebook, Apple, JPMorgan Chase, and PayPal have adopted DMARC to protect their customers and their brand.

Using DMARC, companies gain unprecedented visibility into legitimate and fraudulent mail sent using their domain names. The magic of DMARC is the ability to understand all the different mail streams being sent claiming to be from you—third parties, business units, and threat actors. The overall impact to companies that have adopted DMARC is preservation of brand equity, elimination of customer support costs related to email fraud, and renewed trust and engagement in the company’s email channel.

Email is the #1 way attackers target your customers and email ecosystem.



DMARC—an open standard enabled on 74% of the world’s inboxes—is the only solution that enables Internet-scale email protection and prevents fraudulent use of legitimate brands for email cyberattacks



Introduction to the Basics

What Is DMARC?

DMARC (Domain-based Message Authentication, Reporting and Conformance) is an open email standard published in 2012 by the industry consortium DMARC.org to protect the email channel. DMARC extends previously established authentication standards for email and is the only way for email senders to tell email receivers that the emails they are sending are truly from them. DMARC allows companies that send email to:



Authenticate all legitimate email messages and sources for their email-sending domains, including messages sent from your own infrastructure as well as those sent by third parties.



Publish an explicit policy that instructs mailbox providers what to do with email messages that are provably inauthentic. These messages can either be sent to a junk folder or rejected outright, protecting unsuspecting recipients from exposure to attacks.



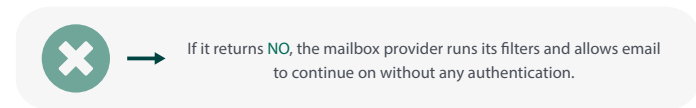
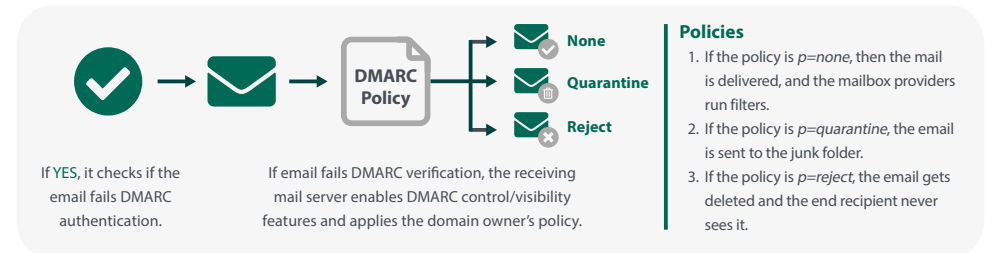
Gain intelligence on their email streams by letting them know who is sending mail from their domains. This data helps companies to not only identify threats against their customers, but also to discover legitimate senders that they may not even be aware of.

What is a DMARC Enforcement Policy?

When you set a DMARC policy for your organization, you as an email sender are indicating that your messages are protected. The policy tells a receiver what to do if one of the authentication methods in DMARC passes or fails.

How it Works

When emails are received by the mailbox provider, the receiver checks if DMARC has been activated for your domain.





The Benefits of DMARC

Why You Should Care

Brand Protection

It is only a matter of time before a criminal will use your domain for their own benefit. Whether the criminal activity is phishing, malware distribution, or nuisance spam, it harms your brand to be associated with these attacks.

Increased Email Deliverability

Even legitimate messages may wind up in the spam folder if the receiver can't tell the good from the bad. By deploying DMARC, you can improve deliverability of your legitimate messages while eliminating the fraudulent ones.

Fewer Customer Service Calls

Customers will not call or send email to ask about phishing messages if they never receive those messages in the first place. One Agari customer was able to redeploy 60 staff members after publishing a reject policy on a highly phished domain.

Visibility Into Cyberattack Risk

Do you know every third-party company sending email on behalf of your company? While third-party senders are needed, each time you provide customer, employee, or partner details to a third-party, you increase the risk of cyberattacks. DMARC enables you to see every third-party sending on your behalf to ensure they comply with email best practices.

The ROI of DMARC



\$19M

Estimated Savings After Deploying DMARC Tool at a Reject Level [Global Cyber Alliance, 2018]



2.4M

Savings with DMARC at Enforcement Level [Forrester, 2019]



5M

DMARC Records Validated by DNS [eSecurity Planet, 2022]



The Bonus to Implementation

DMARC and Inbound Threats

What is BEC?

Business email compromise (BEC) is an inbound threat where attackers impersonate company officials using legitimate domains and send deceptive emails requesting wire transfers to alternate, fraudulent accounts. This often results in successful intrusion and access to victims' credentials.

Characteristics

- Driven by social engineering and digital deception
- Contains no malicious links, malware, or malicious content
- Easily evades the leading secure email gateways and other legacy protections



\$2.4B

Losses from BEC Attacks in 2021

Source: FBI

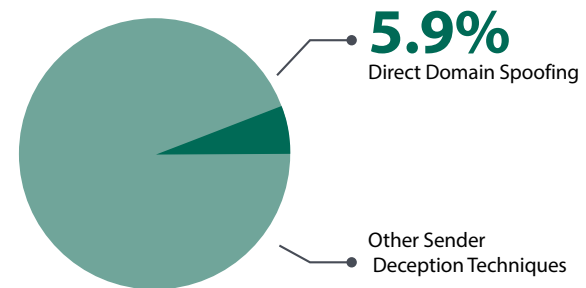
DMARC Addresses a Portion of Inbound Threats

When configured correctly, DMARC stops phishing attacks where the attacker sends an email with a 'From' address that appears to originate from a protected domain. While this makes it ideal for outbound phishing prevention, it can also mitigate certain advanced threats found in inbound traffic sent to employees.

Deception Technique	Addressed by DMARC
Direct/Same Domain Spoofing	✓
Display Name Spoofing	✗
Look-alike Domain Spoofing	✗

Inbound Attacks Prevented by DMARC Alone

Source: Agari



While DMARC partially addresses BEC and sophisticated inbound threats, you need to augment your gateway protections with a comprehensive layer that identifies all forms of sender identity deception.



The Standards

A Closer Look At SPF, DKIM, and DMARC

ABOUT

SPF

(Sender Policy Framework)

SPF is an email authentication standard that allows domain owners to specify which servers are authorized to send email with their domain in the Mail From: email address. SPF allows receivers to query DNS to retrieve the list of authorized servers for a given domain. If an email message arrives via an authorized server, the receiver can consider the email authentic.

DKIM

(DomainKeys Identified Mail)

DKIM is an email authentication standard that cryptographically associates a domain name with an email message. Senders insert cryptographic signatures into email messages that receivers can verify by using DNS-hosted public keys. When verification is successful, DKIM provides a reliable domain-level identifier that can survive forwarding, unlike SPF.

DMARC

(Domain-based Message Authentication, Reporting and Conformance)

DMARC is an email authentication standard that works in conjunction with SPF and DKIM. It brings long-missing features to email, enables senders to gain visibility into how their email domains are used and abused, describes how to combine existing authentication technologies to create secure email channels, and provides receivers with clear directives on how to safely dispose of unauthorized email— all at Internet scale.

EXAMPLE DNS RECORD

example.net. IN TXT
"v=spf1 a mx-all"

selector._domainkey.
example.net IN TXT
"v=DKIM1; k=rsa;
p=public key data"

dmARC.domain.com. IN TXT
"v=DMARC1; p=reject;
rUA=mailto:d@rUA.agari.com;
rUF=mailto:d@rUF.agari.com;"

WEAKNESS

SPF is not ideal for all email use cases and can fail if a message is forwarded. The Mail From domain authenticated by SPF is not easily visible by an email recipient.

DKIM is generally more complex to set up than SPF, requiring a cryptographic signature on each message sent. DKIM will fail when content is modified in transit, like messages sent through a mailing list.

FOR MORE INFO

www.openspf.net

www.dkim.org

www.dmarc.org



The Mechanics

How DMARC Works

The DMARC model uses DNS as the mechanism for policy publication. DMARC records are hosted as TXT DNS records in a DMARC specific namespace. The DMARC namespace is created by prepending “_dmarc.” to the email domain that is to become DMARC compliant. For example, if the email domain “example.com” publishes a DMARC record, issuing a DNS query for the TXT record at “_dmarc.example.com” will retrieve the DMARC record.

The DMARC specification allows senders to publish policy records containing parameters that receivers use to inform the processing of emails that purport to come from the sender’s email domain. The features that DMARC enables are:

Flexible Policies: The DMARC model allows email senders to specify one of three policies to be applied against email that fails underlying authentication checks:

> **p=none:** No policy should be applied, also often referred to as “monitor.” This option is used when senders simply want to collect feedback from receivers.

> **p=quarantine:** Email that fails authentication checks should be treated with suspicion. Most receiving mail systems will deliver these messages to an end user’s spam folder. It could mean increased anti-spam scrutiny or flagging as “suspicious” to end users in some other way.

> **p=reject:** Email that fails authentication checks should be rejected at the receiving mail server. These messages should never reach the end user’s mailbox and feedback will be sent to the party specified in the policy.

Subdomain-Specific Policies: DMARC records can specify different policies for top-level domains vs. subdomains using the p= and sp= tags.

Phased Rollout of Policy: DMARC records can include a “percentage” tag (“pct=”) to specify how much of an email stream should be affected by the policy. Using this feature, senders can experiment with progressively stronger policies until enough operational experience is gained to move to “100% coverage.”

Identifier Alignment Flexibility: The DMARC specification allows domain owners to control the semantics of Identifier Alignment. For both SPF and DKIM generated authenticated domain identifiers, domain owners can specify if strict domain matching is required or if parent and/or subdomains can be considered to match.

Feedback Controls: DMARC records include parameters that specify where, how often, and in which format feedback should be sent to the email domain owner.



The Process

Putting DMARC Into Practice

Domain owners that wish to become DMARC compliant need to perform three activities:

- 1 Publish a DMARC record. To begin collecting feedback from receivers, publish a DMARC record as a TXT record with a domain name of “_dmarc.<your-domain.com>”:

```
“v=DMARC1; p=none; rua=mailto:dmarc-feedback@<your-domain.com>;
```

Doing so will cause DMARC-compliant receivers to generate and send aggregate feedback to “dmarc-feedback@<your-domain.com>”. The “p=none” tag lets receivers know that the domain owner is only interested in collecting feedback. Use the [DMARC record creator](#) on the Agari website to easily create the required text.

- 2 Deploy email authentication for SPF and DKIM.

> Deployment of SPF involves creating and publishing a SPF record that describes all of the servers authorized to send on behalf of an email domain. Small organizations usually have simple SPF records, whereas complex organizations often maintain SPF records that authorize a variety of data centers, partners, and third-party senders. DMARC-supplied aggregate feedback can help identify legitimate servers while bootstrapping a SPF record.

> Deployment of DKIM requires domain owners to configure email servers to insert DKIM signatures into email and to publish public keys in the DNS. DKIM is widely available and supported by all major email vendors. DMARC-supplied aggregate feedback can help identify servers that emit email without DKIM signatures.

- 3 Ensure that Identifier Alignment is met. DMARC-supplied aggregate feedback can be used to identify where underlying authentication technologies are generating authenticated domain identifiers that do not align with the email domain. Correction can be rapidly made once misalignment is identified.

By taking these steps, domain owners can effectively monitor email and make informed security decisions.

Get Started By Creating Records For Your Domain

DMARC

www.agari.com/resources/dmarc

DKIM

www.agari.com/resources/dkim

SPF

www.agari.com/resources/spf

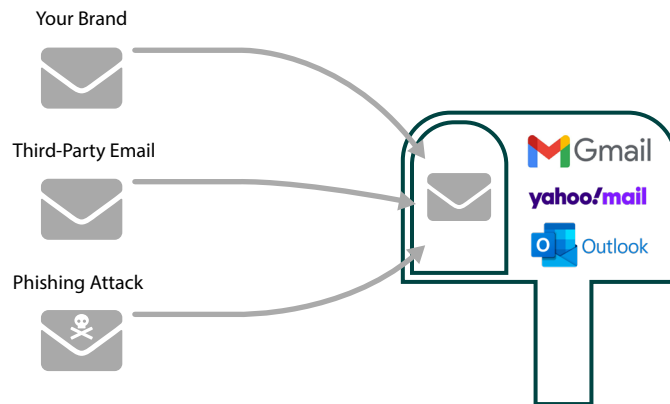


The Big Picture

It's Worth a Thousand Words

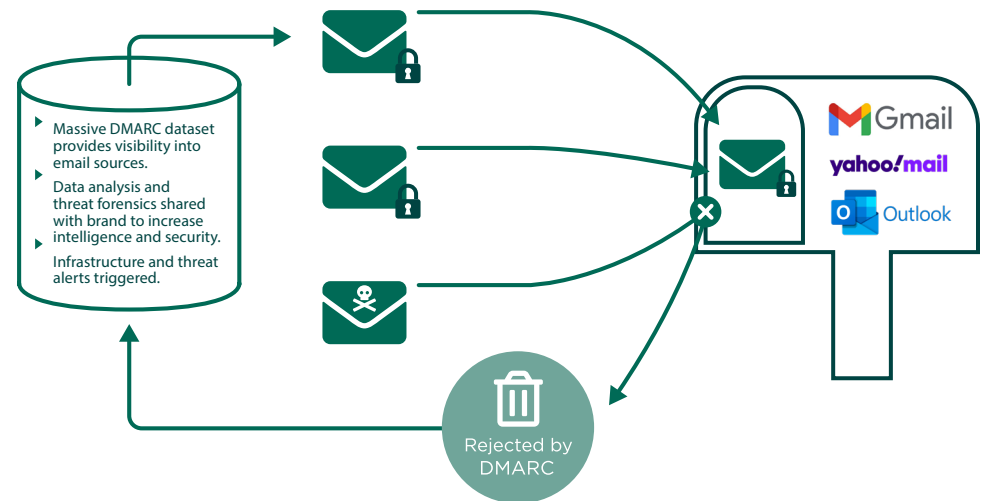
Email Before DMARC

Without DMARC, brands have limited visibility into how domains are being used to send email.



Email After DMARC

DMARC provides visibility into all email traffic and instructs receivers how to handle unauthenticated emails, all outside of the mail flow.



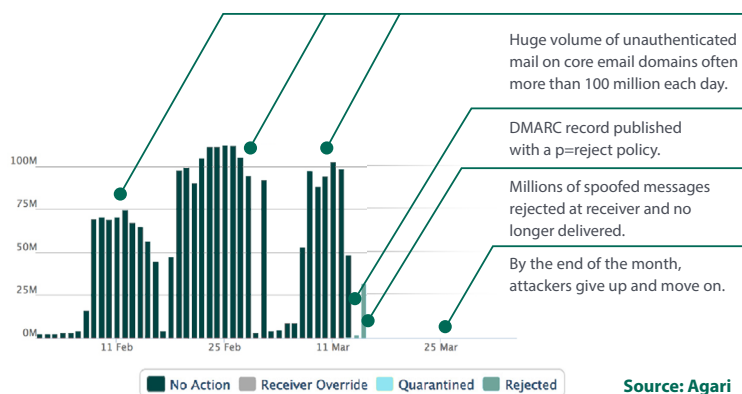


The Results of Implementing DMARC

A Real-World Example

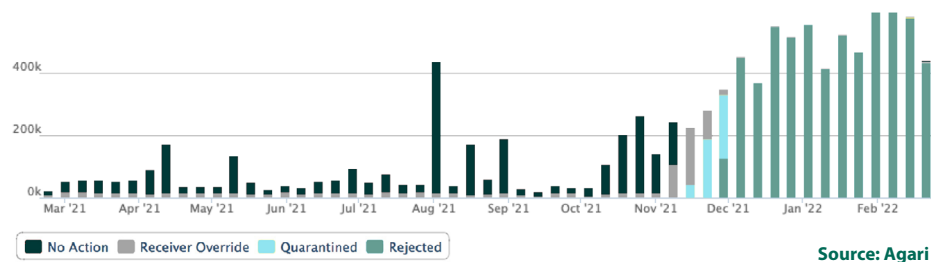
Before and After DMARC Enforcement

The accompanying chart, showing anonymized views of a customer dashboard, highlights the dramatic impact of implementing DMARC. DMARC is so effective at preventing these malicious email campaigns that the bad guys literally give up trying to send malicious email.



Real Agari Customer Example

From March to November, this Fortune 500 large insurance company had no DMARC action policy set (p=none). However in late 2021, they ratcheted up their policy to p=quarantine with Agari which put failed messages into the Spam folder (in yellow). Despite major exploitations by bad threat actors in December- February of 2022 as shown in Agari's threat feed, all of these failed messages were rejected and did not make it to the inbox. These included a deluge of emails coming from unknown IP addresses with low reputation scores from a myriad of irregular countries without host names, but thanks to Agari and DMARC implementation set at the most stringent level these were blocked!

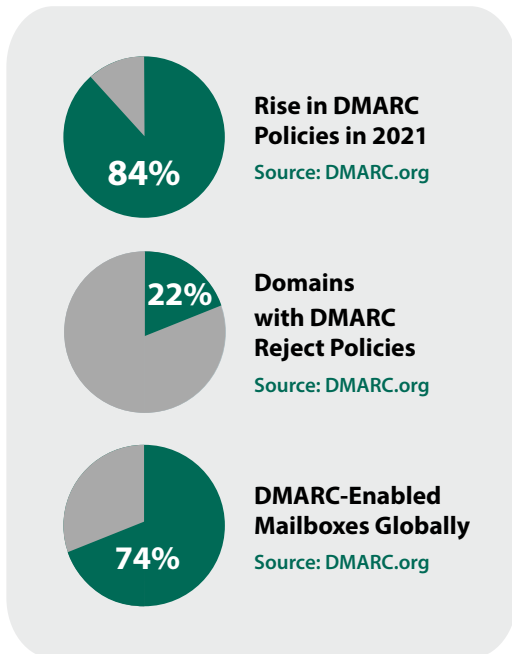




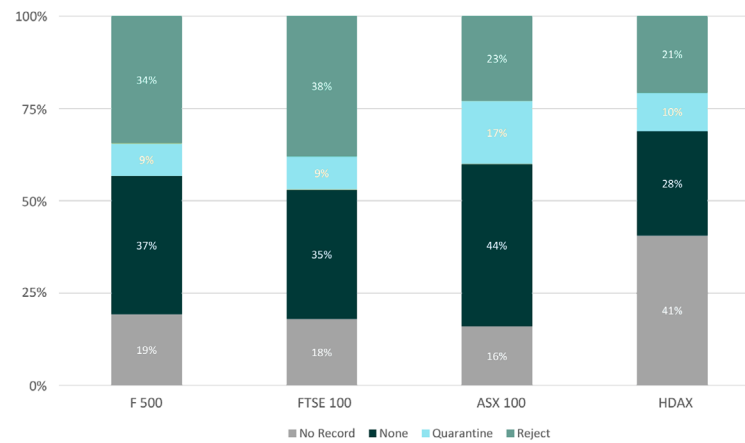
The Numbers Today

DMARC Adoption Worldwide

Strong Consumer Mailbox Adoption



Enforcement Rates of Large Organizations in 2021 Poor Adoption and Enforcement by Large Organizations



Source: Agari

38%
 Financial Times Stock Exchange (FTSE) 100 leads with strongest DMARC enforcement rate

10%
 Jump in Reject level enforcement year over year for Fortune 500 index

1 in 3
 Large organizations in Germany's HDAX index have NO DMARC policy



The Challenge to Implementing DMARC

What Makes DMARC Implementation Hard

Poor Visibility

```

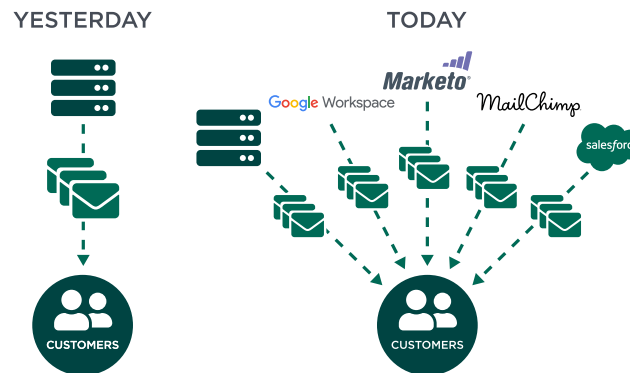
</identifiers>
<auth_results>
<spf>
<domain>subsidiary.com</domain>
<result>fail</result>

```

Most companies don't realize how complex their email ecosystem is until they begin getting aggregate data from DMARC reporting. Standard reporting comes in the form of individual XML files that specify domain names, IP addresses, and authentication details.

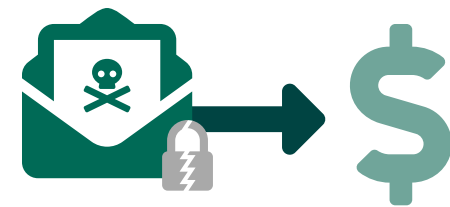
While many tools can parse and visualize this data, making sense of the stream and understanding what subsequent actions to take to improve the authentication status of domains is very difficult and error prone, requiring a deep understanding of email flows.

Discovering and Authorizing Third-Party Senders



The most challenging step of the DMARC journey is understanding all third-party senders and ensuring that legitimate senders are authenticating properly. On average, customers have 64% of legitimate emails sent through third-parties such as Salesforce, Marketo, or MailChimp.

The Cost of "Doing it Wrong"



Despite the emergence of new messaging platforms, email continues to be the most critical vehicle for communication and digital engagement for organizations. Incorrectly configuring authentication can lead to false positives, deliverability issues, and brand damage.

Taking the final step to a p=reject policy can be a daunting prospect if the business impact of undeliverable email is unknown or cannot be predicted.



The Decision

Selecting the Right Vendor

Not all DMARC implementation solutions are created equally, and it can be difficult to interpret some of the marketing claims made by vendors.

In simple terms, there are four main things organizations should look for when evaluating which DMARC partner to use.

1. Proven Scale and Reject Enforcement at the Largest Enterprises

Anything less than an enforcement policy (quarantine or reject) opens the door for cybercriminals to conduct email phishing attacks using your brand to exploit your customers. This is the key business outcome to keep in your sights.

Beware of vendors making promises that guarantee an enforcement policy in a specific number of days.

The reality is that email authentication ties directly to an organization's critical business processes. The process is sometimes simple, sometimes complex, and it cannot be outsourced completely to a third-party vendor.

What to Ask Vendors:

- How long have you been focused on DMARC implementation?
- Did you acquire a tool to meet a product gap?
- What's the largest environment (number of domains) that you've brought to Reject?

2. Automated Discovery and Visualization of Third-Party Senders

Understanding the third-party senders and cloud services sending on your behalf and ensuring legitimate services are properly authenticated are the biggest challenges of achieving DMARC enforcement. This is an essential capability to track sender level authentication progress and monitor new senders. You should not compromise in this area.

What to Ask Vendors:

- Can you automatically generate a visual display (not just IP addresses) of all senders emailing on my behalf?
- How do you discover and validate the senders?



The Decision

Selecting the Right Vendor

3. Adherence to Email Authentication Best Practices with No Vendor Lock-in

DMARC is an open standard developed by pioneers in the email space. Vendors who introduce non-standard approaches and configurations do a disservice to their customers, who will have difficulty migrating off the proprietary system if the need arises.

What to Ask Vendors:

- What non-standard approaches do you use for maintaining SPF records?
- If I move to another vendor to drive my authentication roadmap, how can I migrate the customized settings?
- How is your environment protected from attacks?

Discover Agari DMARC Protection

Visit www.agari.com/products/dmarc-protection/demo for a personalized demo and learn how it can secure your email, protect your customers and partners, and safeguard your overall brand reputation TODAY.

Calculate the ROI of Implementing Agari

As your last line of defense against advanced email attacks, Agari stops attacks that bypass other technologies— protecting employees and customers, while also enabling incident response teams to quickly analyze and respond to targeted attacks.

www.agari.com/resources/roi-calculator/dmarc-protection

4. Support for Enterprise-Class Features

Mature vendors with a proven track record serving the needs of large enterprise and government customers will have the right mix of features and capabilities around reporting, forensics, and ecosystem integration.

What to Ask Vendors:

- Describe the ad-hoc executive level reports you can create. Can you schedule and share reports in CSV and PDF format?
- Do you support role-based and domain-based access control that can map to my organization's process?
- Do you support single sign-on (SSO) access to the application?

FORTRATM

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.