FORTRA

Getting Started with DMARC for Healthcare Organizations

Secure your email.

Stop phishing.

Protect your brand.

The History

Introduction

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

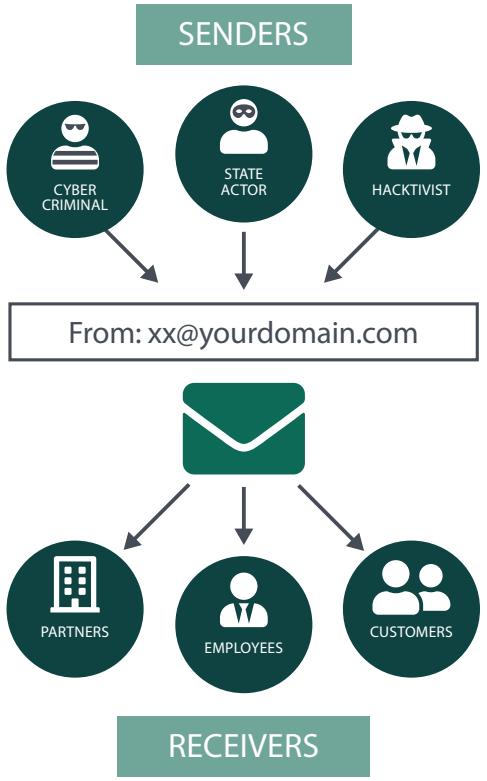
Prior attempts at security have failed to solve email's fundamental flaw – anyone can send email using someone else's identity. This flaw has put the power of the world's most admired healthcare and public health brands in criminal hands. Through email, criminals can use almost any brand to send spam,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

Many of the most respected healthcare brands in the world, including Aetna, Merck, Blue Shield of California, and more have adopted DMARC to protect their customers and their brand.

Using DMARC, healthcare organizations can 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.

DMARC – an open standard enabled on 70% of the world's inboxes and is the only solution that enables Internet-scale email protection and prevents fraudulent use of legitimate brands for email cyberattacks.

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



Threat Rate	56.96% Malicious Emails	92.83% Domain Targeted

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.

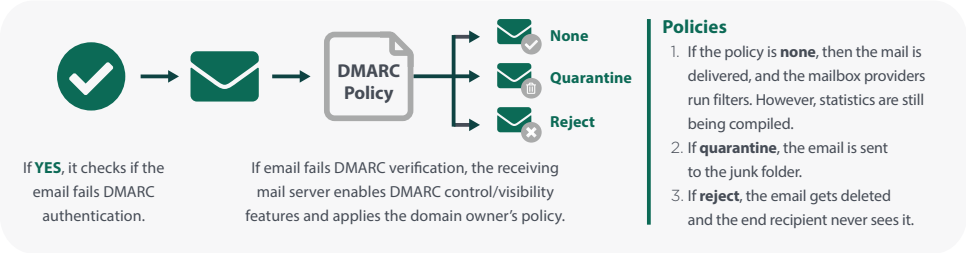
Gain intelligence on their email streams by letting them know who is sending mail from their domains. This data helps companies to not only identify threats against their customers, but also to discover legitimate senders that they may not even be aware of.

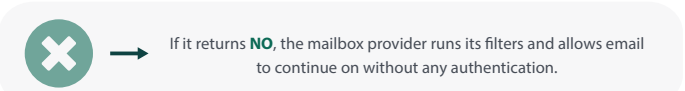
What is a DMARC Enforcement Policy?

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 Believers

Early Adopters Pave the Path

2.5 Billion Mailboxes Worldwide are DMARC-Enabled

DMARC SENDERS

Santander, NETFLIX, ups, JPMorganChase, aetna, box, WESTERN UNION, citi, UNITED STATES POSTAL SERVICE, PayPal, D&B, DHL, livingsocial, usbank, LinkedIn, CapitalOne, facebook, ADP, Skrill

DMARC RECEIVERS

Google, YAHOO!, Microsoft, Aol., COMCAST, SBC, at&t, BT

Who Endorses DMARC

INDUSTRY ASSOCIATIONS

OTA Online Trust Alliance, M³AAWG Messaging Malware Mobile Anti-Abuse Working Group, BITS, DMARC, Financial Services Information Sharing and Analysis Center, NH-ISAC National Health - ISAC

GOVERNMENT AGENCIES

NIST, Homeland Security, GOV.UK

The Benefits

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

326%
Return on Investment

$4M
Increased Return on Customer Engagement

$1.1M
Reduced Need for Customer Support

$718K
Reduced Cost of Cybersecurity Insurance

10%
Rise in Response Rate to Email Campaigns

The Bonus

DMARC and Inbound Threats like BEC

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

The Impact

$2.4B

Losses from BEC Attacks in 2021

Source: FBI

DMARC Addresses a Portion of Inbound Threats

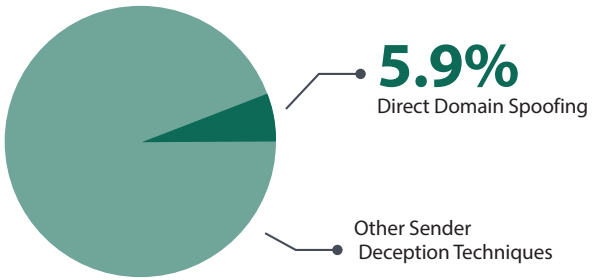
When configured correctly, DMARC stops phishing attacks where the attacker sends an email with a 'From' address that appears to originate from a protected domain. While this makes it ideal for outbound phishing prevention, it can also mitigate certain advanced threats found in inbound traffic sent to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

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.

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

Inbound Attacks Prevented by DMARC Alone

Source: Agari
Sept 2017



The Standards

A Closer Look

	SPF (Sender Policy Framework)	DKIM (DomainKeys Identified Mail)	DMARC (Domain-based Message Authentication, Reporting and Conformance)
ABOUT	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 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 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.

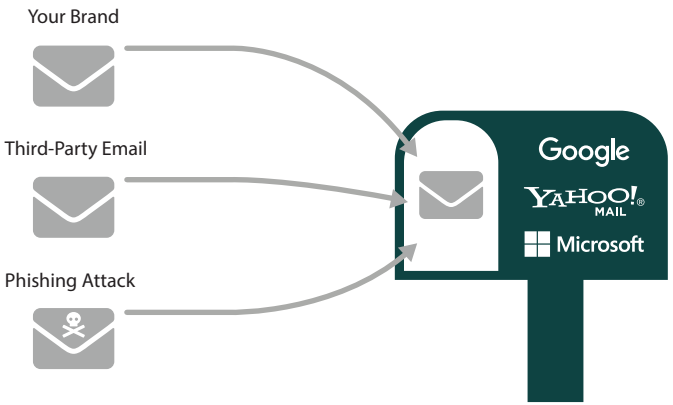
By taking these steps, domain owners can effectively monitor email and make informed security decisions.

The Big Picture

It's Worth a Thousand Words

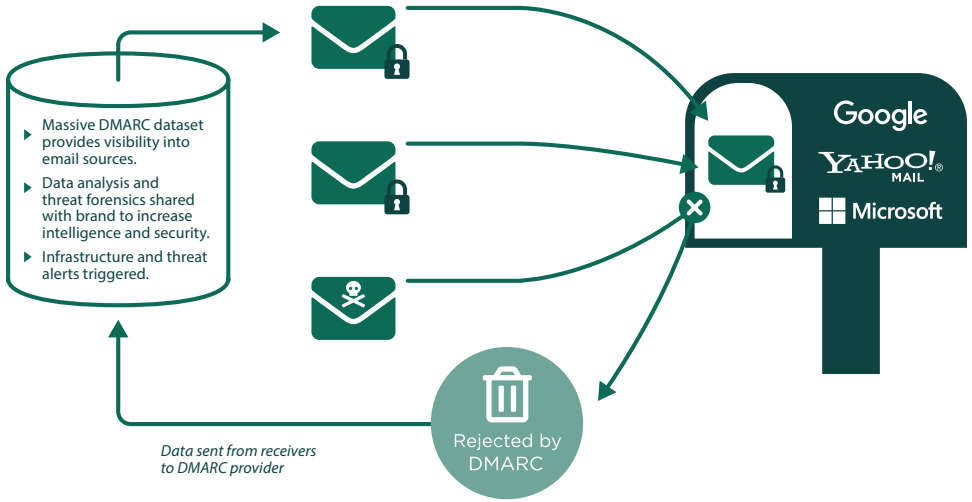
Email Before DMARC

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.

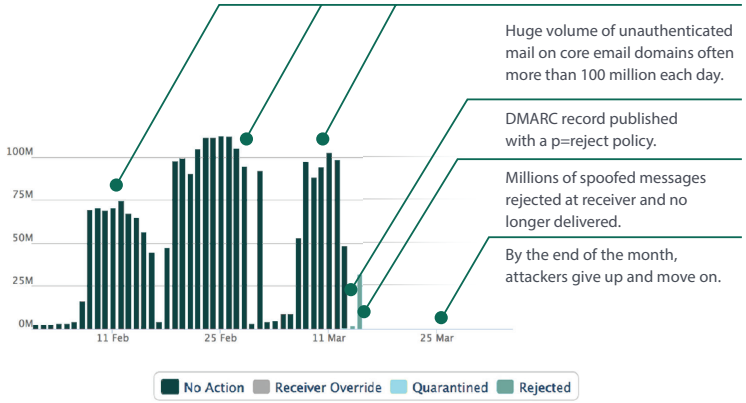


The Results

A Real-World Example

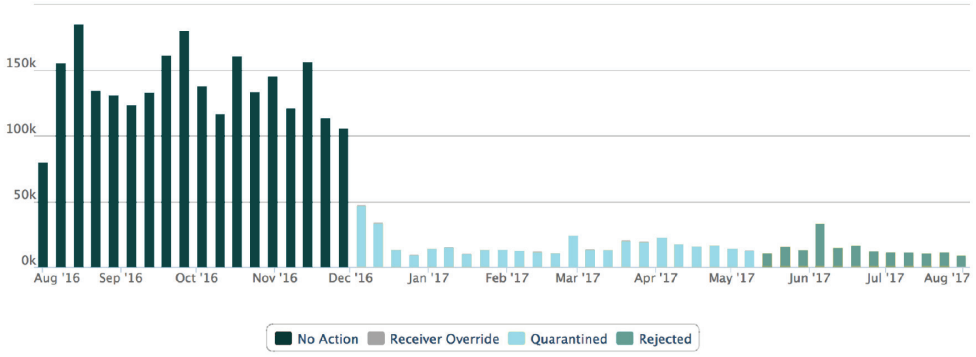
Before and After DMARC Enforcement

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.



The Best Practice: Gradually Moving To Enforcement

This next chart depicts another campaign targeting new domains. Here, the customer employed a gradual adoption of tighter DMARC policies, just as DMARC was designed to be deployed. Initially, unauthenticated mail volume surpassed 100,000 to 150,000 messages per day. After a Quarantine policy, this was cut to 50,000 or less. The policy was tightened further to a Reject policy, which practically eliminated the volume of unauthenticated email.

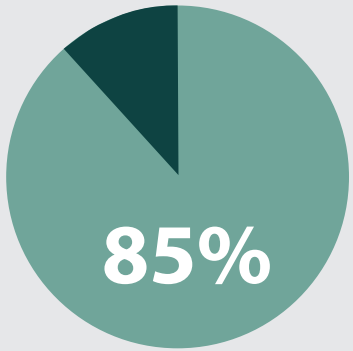


The Numbers Today

DMARC Adoption in Healthcare

The Good News: Strong Consumer Mailbox Adoption

DMARC ENABLED MAILBOXES IN THE US



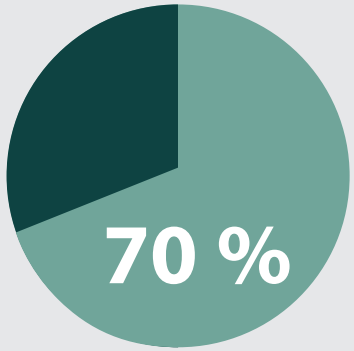
Source: Facebook via DMARC.org

DOMAINS WITH DMARC REJECT

> 80,000

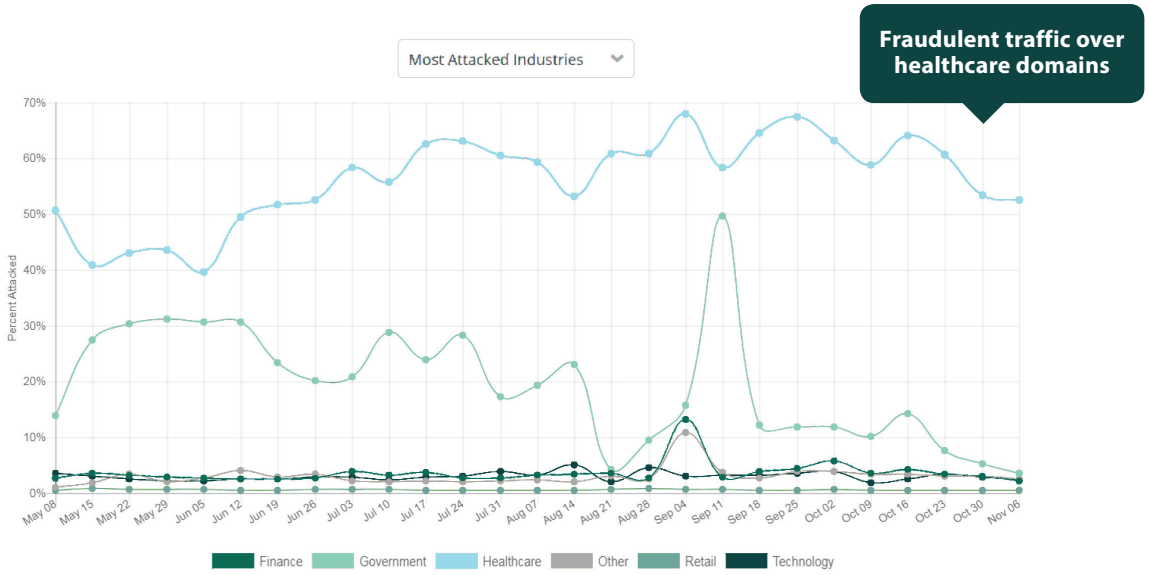
Source: Google

DMARC ENABLED MAILBOXES GLOBALLY



Source: DMARC.org

Healthcare Is The Most-Attacked Industry For Fraudulent Email[1]



SOURCES

[1] Agari. Analyze the latest email fraud stats for healthcare and other sectors at www.agari.com/email-threat-center/

[2] Public DNS record analysis on corporate healthcare website domains.

[3] Anonymous adoption data provided by NH=ISAC.

POOR GLOBAL ADOPTION IN HEALTHCARE[2]

- **77%** NO DMARC policy
- **21%** Monitor-only policy (doesn't prevent email abuse)
- **2%** Quarantine or Reject policy to folder or block messages that fail authentication

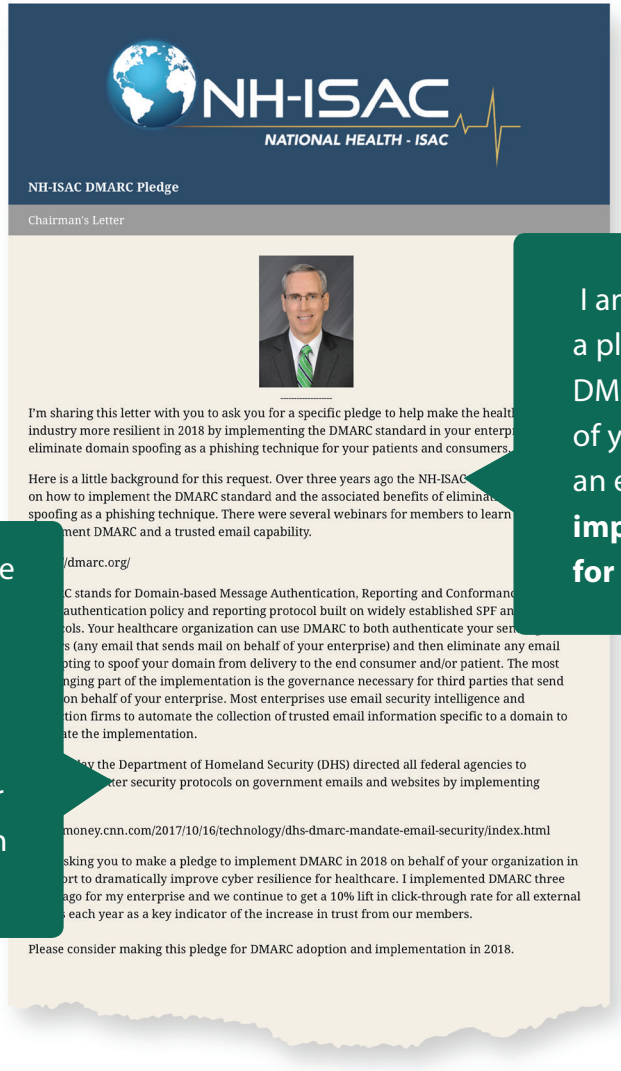
POOR NH-ISAC ADOPTION[3]

- **70%** NO DMARC policy
- **27%** Monitor-only policy (doesn't prevent email abuse)
- **3%** Quarantine or Reject policy to folder or block messages that fail authentication

The Pledge

Commit to making email safer for patients, customers, and employees

On October 16th, 2017, the Department of Homeland Security (DHS) directed all federal agencies to implement better security protocols on government emails and websites by implementing DMARC. That same week, Jim Routh, Chairman of the NH-ISAC, issued a letter enlisting NH-ISAC member to take a "pledge" to implement DMARC.


NH-ISAC
NATIONAL HEALTH - ISAC

NH-ISAC DMARC Pledge

Chairman's Letter

I'm sharing this letter with you to ask you for a specific pledge to help make the healt
industry more resilient in 2018 by implementing the DMARC standard in your enterp
eliminate domain spoofing as a phishing technique for your patients and consumers.

Here is a little background for this request. Over three years ago the NH-ISAC
on how to implement the DMARC standard and the associated benefits of eliminat
spoofing as a phishing technique. There were several webinars for members to learn
ment DMARC and a trusted email capability.

/dmarc.org/

C stands for Domain-based Message Authentication, Reporting and Conformanc
authentication policy and reporting protocol built on widely established SPF an
ols. Your healthcare organization can use DMARC to both authenticate your ser
s (any email that sends mail on behalf of your enterprise) and then eliminate any email
pting to spoof your domain from delivery to the end consumer and/or patient. The most
nging part of the implementation is the governance necessary for third parties that send
on behalf of your enterprise. Most enterprises use email security intelligence and
tion firms to automate the collection of trusted email information specific to a domain to
te the implementation.

ey the Department of Homeland Security (DHS) directed all federal agencies to
ter security protocols on government emails and websites by implementing

money.cnn.com/2017/10/16/technology/dhs-dmarc-mandate-email-security/index.html

sking you to make a pledge to implement DMARC in 2018 on behalf of your organization in
ort to dramatically improve cyber resilience for healthcare. I implemented DMARC three
ago for my enterprise and we continue to get a 10% lift in click-through rate for all external
each year as a key indicator of the increase in trust from our members.

Please consider making this pledge for DMARC adoption and implementation in 2018.

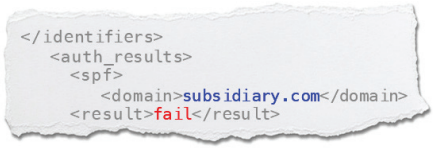
I am asking you to make a pledge to implement DMARC in 2018 on behalf of your organization in an effort to **dramatically improve cyber resilience for healthcare**

I implemented DMARC three years ago for my enterprise and **we continue to get a 10% lift in click-through rate** for all external emails each year as a key indicator of the increase in trust from our members

The Challenge to Implementing DMARC

What Makes DMARC Implementation Hard

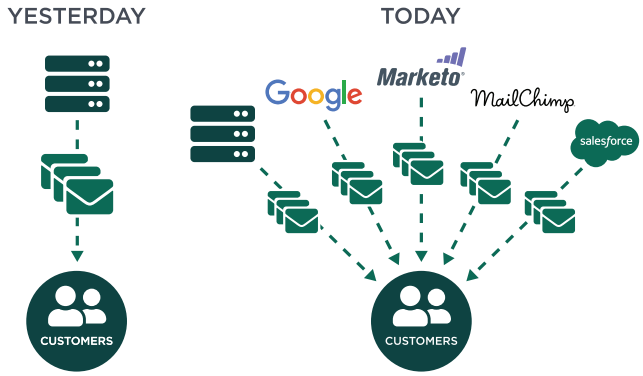
Poor Visibility



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.

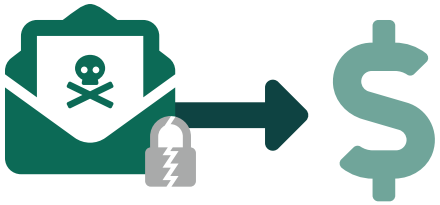
While many tools can parse and visualize this data, making sense of the stream and understanding what subsequent actions to take to improve the authentication status of domains is very difficult and error prone, requiring a deep understanding of email flows.

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 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 to Deliver on the DMARC Promise

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 and reputation to exploit your customers. This is the key business outcome to keep in your sights. Beware of vendors making promises like "we guarantee you will get to Reject in 90 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 3rd 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?

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?

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 eports 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?
- Do you have an app that pulls relevant information from brand/domain events into Splunk?

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.

fta-ag-gd-1022-r1-79d