FORTRA™

SOLUTION BRIEF (AGARI)

Implementing DMARC in the Federal Government

The key to eliminating phishing and safeguarding email communication.

The Problem

Email is the #1 way attackers target citizens and government employees.

WHY IT WORKS

Email lacks built-in authentication

Attackers can easily spoof or impersonate anyone in your organisation using free tools.

Attackers need to be right just once

With billions of emails hitting government inboxes, odds are in the attacker's favor.

Email gateways can't solely solve the problem

Attackers rely on social engineering tactics and identity deception, not malicious content or URLs that traditional tools were built to detect.

WHAT IS DMARC?

DMARC (Domain-based Message Authentication Reporting & Conformance) is an open email authentication protocol, established in 2012 by organizations including Google, Microsoft, Agari, PayPal, and others to protect the email channel. DMARC is the best way for email senders and receivers to determine whether or not a given message is legitimately from the sender, and what to do if it isn't.

"Business Email Compromise (BEC) attacks represent more than 50% of all incidents and this number has been doubling each year since 2017, which makes it especially noteworthy."

— Verizon 2023 Data Breach Report

"Phishing...continue[s] to present threats to both the federal government and public at large."

— US Federal Information Security Management Act (FISMA)

GOVERNMENT AGENCIES WITH DMARC ADOPTION

UNITED STATES POSTAL SERVICE

FDIC

U.S. Customs and Border Protection

The Solution

DMARC functions like an 'identity check' for your agency. It prevents spammers and criminals from hijacking your valid organization domain names and brand for email.

BENEFITS OF DEPLOYING DMARC FOR YOUR AGENCY

Stop email phishing attacks using your agency's reputation: Agencies reduce the likelihood that their domains and brand will be used in an attack.

Reduce account takeover risk:
By preventing delivery of phishing and malware-laden messages directed at your employees or constituents, you can reduce the number of account takeovers.

Increase email deliverability:
By deploying DMARC, you ensure that legitimate email from your agency gets delivered and is not blocked at the receiver.

Gain visibility into cyberattack risk:
Do you know every third party company that sends email on behalf of your agency? DMARC provides this critical visibility, allowing you to ensure that anyone sending on your behalf complies with email best practices.

THE FEDERAL PERSPECTIVE

The Department of Homeland Security (DHS) has mandated adoption of DMARC on all government agency email domains.

DMARC (and email authentication) is evolving into a key metric that impacts the **FISMA** scorecard against your agency.

NIST recommends using DMARC authentication tools to provide protection against phishing (SP 800-177, Trustworthy Email, Section 4.6).

A DMARC Primer

DMARC is a complex and potentially lengthy journey, requiring vast visibility and expertise. Often customers in the public sector find themselves stagnated in their authentication progression, lacking in the tools they need to reach *"p=reject"*. What steps does my agency need to take to use DMARC?

Implement Authentication Standards

The DMARC protocol builds on existing standards like Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM).

Authorize/Validate Approved Senders

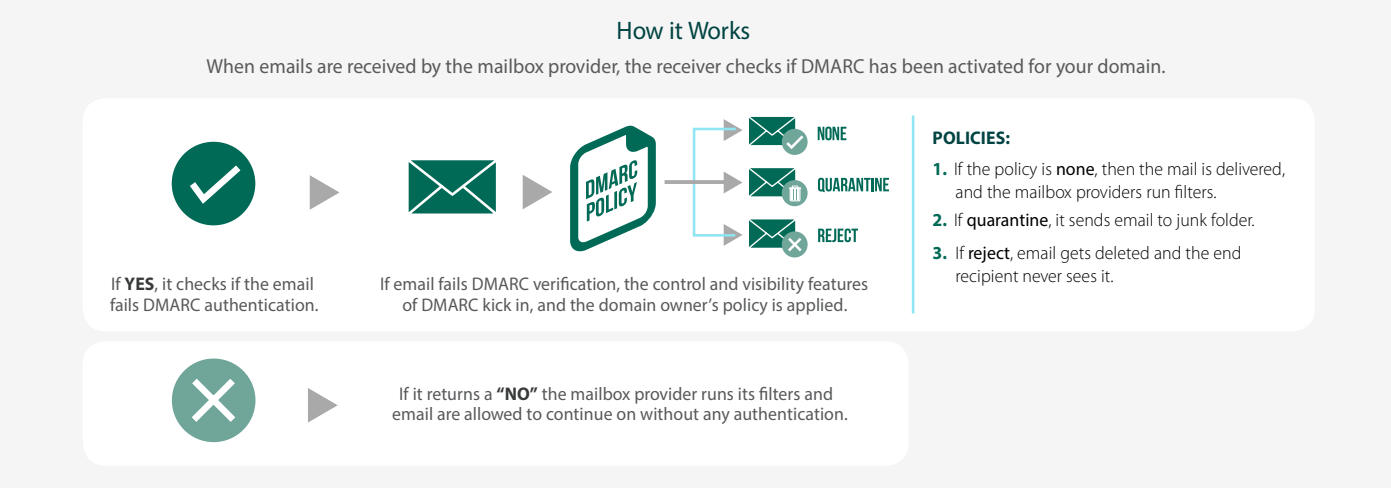
You need to understand and authenticate all legitimate email messages and sources for your email-sending domains, including owned and third party domains. it is crucial to ensure you don't block legitimate mail, that is senton your behalf.

Set DMARC Enforcement Policy

This is a key milestone in the DMARC journey. Publishing an explicit policy tells mailbox providers what to do with email messages that are determined not to be legitimate. This is how you can block all fraudulent emails before they reach employees, constituents, and citizens at large.

What is a DMARC Enforcement Policy?

When you set a DMARC policy for your agency 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.



Here's a typical policy in DNS. Note that this domain is configured with a policy of Reject DMARC record for agari.com:

```
v=DMARC1; p=reject; sp=reject; ri=3600; rua=mailto:agari-data@rua.agari.com;
ruf=mailto:agari-data@ruf.agari.com; fo=1
```

How Do I Get Visibility and Reporting from DMARC?

Once your DMARC policy is implemented, you will start to to receive thousands of reports every day, depending upon the number of emails your organization sends. Because it's difficult to process the reports manually, you can work with a commercial vendor to display and process the data. Commercial vendors such as Agari can help with DMARC policy creation and hosting, third-party sender identification and alignment, and ongoing visibility as you progress through your DMARC implementation. In fact, Fortra's Agari DMARC Protection ensures companies reach Reject confidently and securely, boasting an enforcement rate of 78%.

Learn More: www.agari.com/products/dmarc-protection

FORTRA™

Fortra.com

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.