FORTRA™

DATASHEET *(Cybersecurity)*

# Post-Enforcement Advantages of Agari DMARC Protection

## Moving from Maintaining to Monitoring

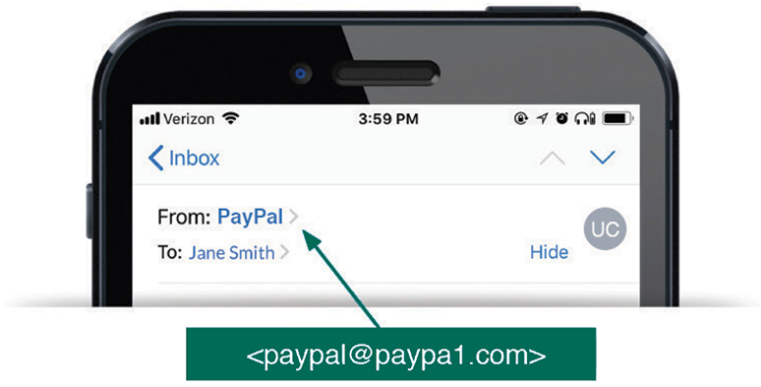
After implementing DMARC with a p=reject policy, the next phase of active monitoring is just as crucial to ensuring your brand and customer base remains protected from abuse as cybercriminals change tactics. Agari DMARC Protection remains a key component in helping monitor changes after email authentication has been implemented, and achieves this through a proven process, including:

### Managing New Third-Party Senders

- Enables control of third-party SaaS applications and cloud services sending on your company's behalf
- Automatically identifies sender domains and IP addresses for you to track and approve on your personalized Threat Feed

### Gaining Visibility into New Attack Vectors

- Protects against brand abuse by continuously identifying, monitoring, and taking malicious domains offline quickly and completely
- Continues to monitor as cybercriminals try new tactics, such as spear phishing, to trick you and your customers




### AT A GLANCE

After reaching a DMARC enforcement policy, Agari DMARC Protection continues to provide immense value to customers.

**BENEFITS**

**Improves customer trust**
by protecting your brand from being used in phishing attacks.

**Decreases time to reject**
by automating implementation.

**Maximizes marketing efficacy**
and improves email engagement with trusted communications.

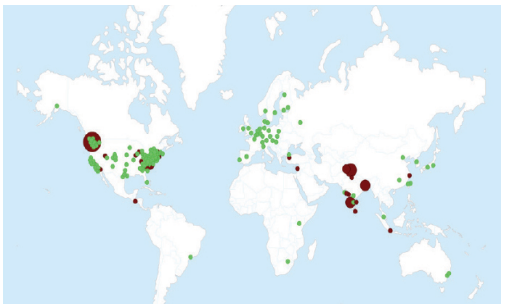
**Reduces operational costs**
associated with email channel management.

***"Email is the communications channel for the top cybersecurity threats impacting customers, employees, and suppliers. By protecting the email channel with Agari, we are improving our security posture enormously—protecting our brand and helping our business build trusted relationships with our customers."***

Manager of IT Security and Risk Management

## Mitigating Threats to Further You Towards Your DMARC Destination

- Uses DMARC threat data to block any inbound email that is outside of your sender inventory
- Enables intelligence sharing through Failure Sample DMARC data and has the ability to take down phishing sites and infrastructure



## Leveraging Intelligence to Thwart Threats & Attacks

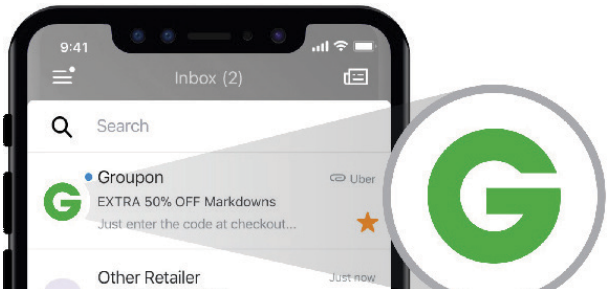
- Supports rapid remediation with takedown vendors after identifying suspicious or malicious URLs, shutting down phishing sites
- Seamlessly feeds threat data to your SIEM or SOAR platform, such as Splunk and Microsoft Sentinel, over open APIs

## Ensuring Compliance & Reporting through an Executive Dashboard

- Clearly and efficiently identifies senders, logos, domains, and IP addresses for compliance and laws surrounding your customers' confidential data
- Automatically provides analytics and trend reporting to industry peers and executives for substantiation of ROI

## Providing a Bevy of Brand Impressions

- Implements BIMI, or Brand Indicators for Messaging Identification, so your outgoing email has your logo next to the Sender "From" address
- Provides an immediate visual indication of authentication from the sending domain to the recipient, instilling trust in your brand




## Continuing Your Email Security Journey

Implementing DMARC is a great first step in protecting your customers, partners, and employees from cyberattacks, but it will not prevent all email-based threats. Improve your security posture with Agari DMARC Protection and stop advanced email threats in their tracks while remediating phishing attacks.

Request your personalized demo today.

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.