FORTRA

SOLUTION BRIEF

Agari Automation and Hosting Features

Email authentication without limits.

The Email Authentication Challenge

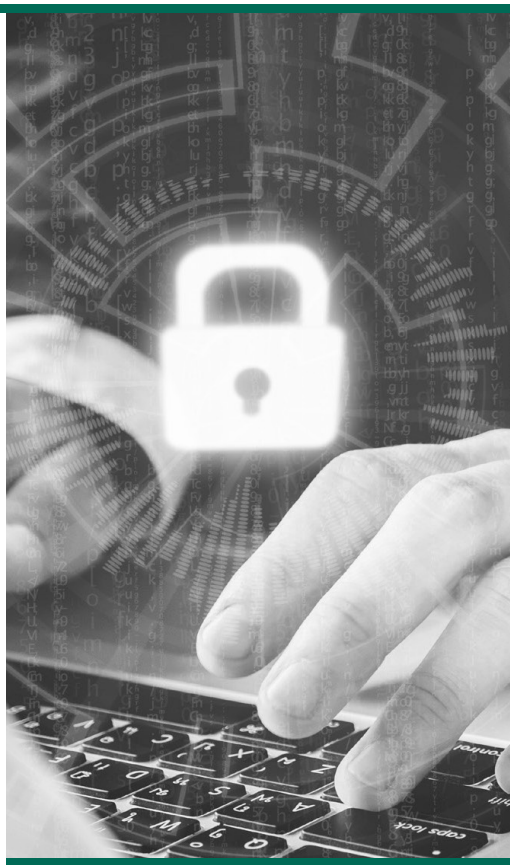
Email is the #1 way attackers target an organization's customers and email ecosystem. DMARC authentication, specifically with an enforcement policy of Reject, is the single most effective way to close this vulnerability inherent to email. While the premise of authentication is straightforward, organizations can encounter roadblocks and challenges along the way to an enforcement policy. These include:

The "many sender" problem: Email environments are often complex, comprised of many domains associated with dozens of legitimate senders, such as Salesforce and Marketo, along with many illegitimates ones—spammers, cybercriminals, and others looking to profit from your brand.

Organizations need a painless way to understand and manage the domains used by their email ecosystem, including their own internal and third-party senders.

Ongoing configuration and record maintenance in DNS: The workflow and configuration of DMARC authentication is intricately tied into legacy DNS systems. In many organizations, access and change control around DNS can be problematic. The frequency with authentication-related records needing to be updated combined with the lack of robust error handing within DNS itself often complicates and extends DMARC projects.

The cost of "doing it wrong": 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. This brief summarizes how the automation features and hosting options with Agari DMARC Protection solves these challenges.

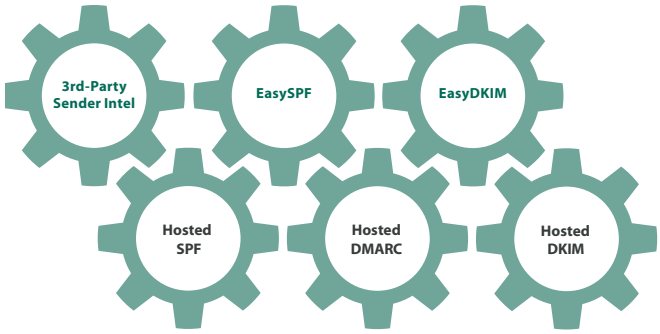


"With Agari, we prevent the delivery of thousands of fraudulent emails every month, triggered by cybercriminals who attempt to use our brand or phish our members."

Ben Schoenecker
Senior Security Engineer,
AllSouth Federal Credit Union

The Agari Solution

Managing this kind of complexity requires powerful, smart tools that organize the various sender, brand, and infrastructure relationships for you. Whether you are creating your own SPF and DMARC records or having Agari host them, Agari's automation features will get you to enforcement quickly.



Automation Features in Agari DMARC Protection

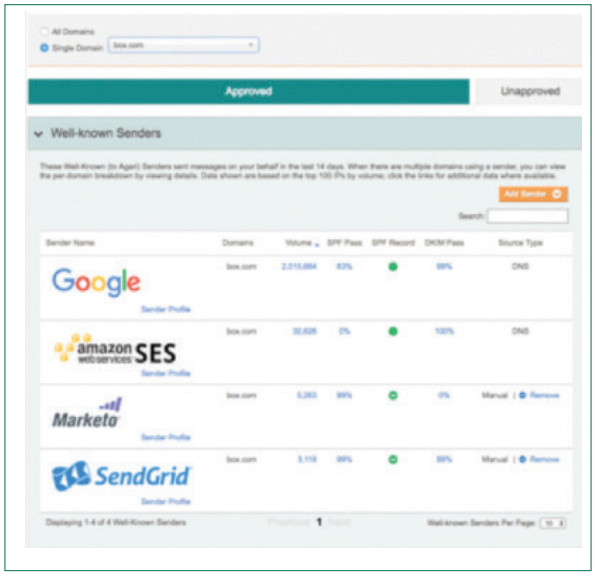
Automation Features

3rd-Party Sender Intelligence (3PSI)

For many organizations, cloud-based email services such as Salesforce, Marketo, or Epsilon represent the majority of email sent to customers and partners. Getting visibility into these third parties is a must before organizations can protect customers from phishing attacks; but manually matching brands with IP address and domains is a long, arduous process and is not scalable.

HOW IT WORKS:

3PSI identifies who is communicating with your customers using your brand. It provides one place to view and manage sender domains and unknown IP addresses. This, in turn, enables businesses to easily identify and authorize legitimate email communications and block malicious ones.



BENEFIT:

3PSI enables businesses to easily identify and authorize legitimate email communications, block malicious emails, and protect customers, partners, and employees from advanced email attacks. This, in turn, improves customer response to email campaigns and protects your brand.

EasySPF

Sender Policy Framework (SPF) is one type of DNS entry that assures email from a sender is actually from that sender and it is a critically-important component of DMARC integration. However getting to enforcement using a manual process is difficult, costly, and error-prone.

HOW IT WORKS:

On a per domain basis, Agari's EasySPF enables enterprises to quickly and accurately inventory all of their senders and associate the approved ones with each domain.

BENEFIT:

EasySPF automates the process of building SPF records, simplifying and accelerating the implementation of DMARC.

EasyDKIM

DKIM is another authentication-oriented text record in DNS. DKIM, which leverages public keys and depends on alignment with pertinent details within the SPF record, verifies message integrity, ensuring that a message's content has not changed from the moment the message left the initial mail server. As policies and selectors vary with different senders, DKIM can be hard to manage and keep updated.

HOW IT WORKS:

EasyDKIM solves the challenges around DKIM management by providing DKIM situational awareness and tracking tools, automated DKIM selectors detection for senders, and enabling key rotation best practices.

BENEFIT:

Automatically monitor your current DKIM environment and quickly align your senders to stay in compliance with cybersecurity best practices.

"I really should be rotating my keys but it's so hard to keep track of. Something like this does the heavy lifting for me."

Fortune 1000 Multinational Software Company

"I've been manually updating a spreadsheet for four years to do what this feature does automatically."

Fortune 1000 Multinational Global Manufacturer

Hosting Features

There are often many hidden costs to managing SPF, DKIM, and DMARC services. However, choosing a hosted deployment with Agari eliminates these additional costs by providing 24/7/365 resources and support. Agari hosted solutions combined with Agari automation services enable proactive detection of SPF, DKIM, and DMARC with your legitimate senders and monitors any irregularities to ensure nothing impacts the productivity of your business. All Agari resources possess the required skill set for monitoring and administrating your DMARC solution without need for you to hire any additional resources.

Top Benefits of Agari Hosted Solutions

AGARI HOSTING ADVANTAGE OVERVIEW

- Delivers the fastest possible business outcome for your purchase.
- Guarantees 100% error free email delivery for authenticated domains, new domains, and new senders.
- Eliminates additional investment of customer supplied resources.
- Offers unlimited and anytime support from our specialists through live chat, support tickets, or phone

Hosted SPF

Corporations often don't have the time (or the expertise to) build and host their own SPF records as part of the email authentication process.

HOW IT WORKS:

When Agari hosts the SPF record we completely take over the DMARC authentication process for all senders, including third-party ones. This is an alternative to using EasySPF to build your own record. It is an optional feature and organizations who don't want to be locked into a given vendor can host their own.

BENEFIT:

Agari assumes the responsibility of creating and hosting the SPF record, which is a critical step in the DMARC enforcement process. This means with a simple DNS change, companies are relieved from the burden of doing it themselves and ensured that the job is done correctly.

Hosted DKIM

For those organizations who prefer a full-service implementation, they can turn over DKIM record management to Agari.

HOW IT WORKS:

As with SPF and DMARC records, organizations can choose to save the DNS management, infrastructure, and fulltime employee costs related to authentication by taking the DKIM management out of their environments.

BENEFIT:

Have Agari host your DKIM to avoid the hassle and risk of DNS record changes. Free your DNS and email administrators to focus on other more urgent matters.

Hosted DMARC

For those organizations who prefer a full-service implementation, they can turn over the DMARC record management to Agari.

HOW IT WORKS:

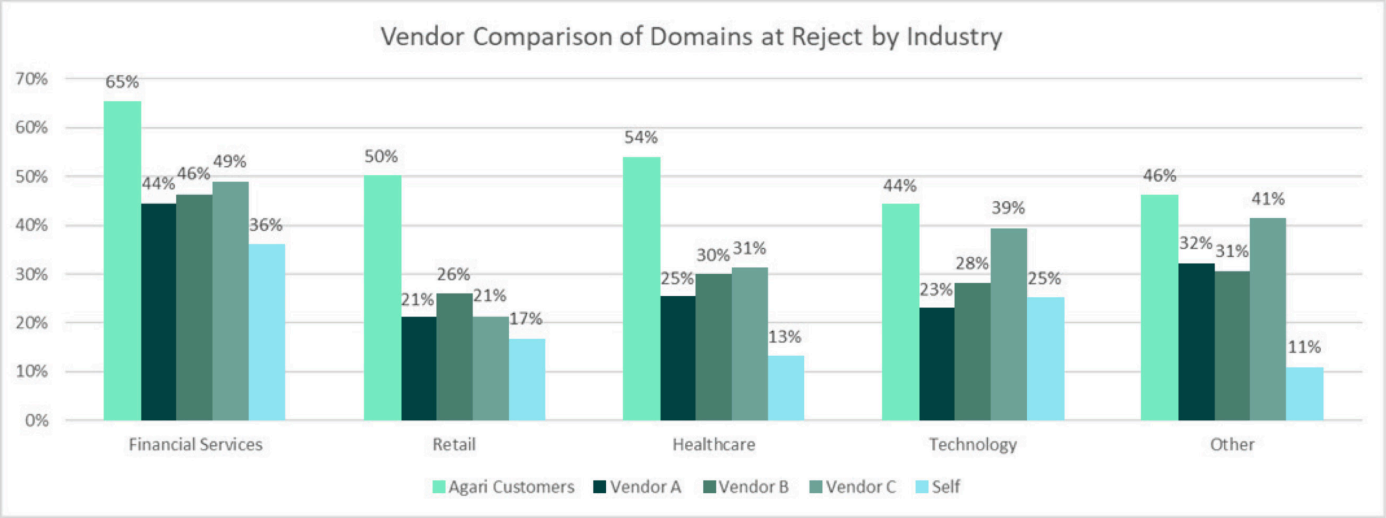
Organizations can use the Agari Hosted DMARC feature whether they have no DMARC record or have one that they are currently hosting themselves. The process is as easy as selecting the domains that currently lack a DMARC and clicking a button to have Agari host them. This feature may be paired with our new Hosted SPF feature to streamline authentication.

BENEFIT:

Hosted DMARC simplifies the initial DMARC implementation process as well as streamlines sender updates as they occur.

Getting To Enforcement

Vendors often claim to offer automation and ease of DMARC implementation, but when one looks at the actual protection ratios, the truth emerges. Agari has more domains at reject than any other vendor. Organizations serious about blocking phishing shouldn't settle for a vendor who has most of their customers stalled at or monitor-only mode.



The Fortra Advantage

Agari combines its own third-party sender knowledge and automation with intelligence-fed tools that let you authenticate your organization's legitimate email, blocking unauthorized emails from reaching your customers. Agari has brought more customer domains to a Reject policy than any other vendor. And when criminals switch tactics to employing look-alike or cousin domains, our Look-alike Domain Defense alerts you to these messages spoofing your brand and allows you to detect the malicious URLs so that you can disable the attack. Finally, Agari offers fully hosted authentication, enabling the fastest path to enforcement while freeing your in-house resources to work on other priorities.

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.