AGARI

SOLUTION BRIEF

Agari Business Fraud Protection™

Prevent attackers from abusing your corporate email domains.

Corporate Domains Are Under Attack

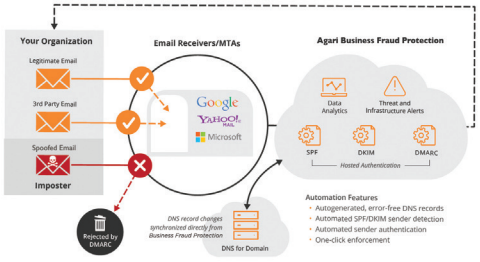
Your organization's corporate domain is one of its most valuable assets. Left unprotected, it is easy for cybercriminals to spoof your domain and attack your customers, partners, and employees. Using any email address at your company (such as payments@company.com), criminals can send your customers fake invoices, trick them into paying, and then make off with the proceeds. In other cases, attackers will commit fraud in your name by impersonating an executive within the company, legal counsel, or a human resources director. Using these names, attacks can often get access to private information such as upcoming mergers or employee W2s.

Domain spoofing—when an attacker appears to use a company's domain to impersonate an employee or the company itself—is commonly used to execute business email compromise (BEC) attacks such as these. Thankfully, these threats can be stopped by implementing

email authentication.

Protect Your Corporate Domains With Automated Email Authentication

Agari Business Fraud Protection stops phishing attacks targeting your employees, customers, and supply chain by automating the process of DMARC email authentication and enforcement. Implementing a DMARC enforcement policy of "Reject" protects your email from being spoofed and used in email attacks. Agari's unique, automated approach to email authentication provides organizations with a simple and effective solution to prevent abuse of corporate email domains.



Agari analyzes two trillion emails per year claiming to be from domains across the world's largest cloud email providers. Combining Business Fraud Protection tools with 3rd party sender knowledge, Agari lets you authenticate your organization's legitimate email, thereby blocking unauthorized email from reaching your customers, partners, and employees. Once DMARC authentication is in place, Agari continuously monitors your environment to ensure authentication remains resilient as your email infrastructure evolves to meet demand.

AT A GLANCE

Agari Business Fraud Protection automates DMARC email authentication and enforcement to prevent corporate domains from being used to defraud B2B customers, business partners, and employees.

BENEFITS

Protect employees by stopping domain spoofing and business email compromise attacks.

Prevent fraud losses by preventing invoice scams from vendors and partners.

Increase trust and protect the value of your brand with your B2B customers

Ensure compliance with corporate email usage policies.

THE AGARI ADVANTAGE

Fully hosted DMARC deployment reduces administration and management burden.

Domain spoofing protection prevents BEC attacks targeting vulnerable customers, partners, and employees.

Email cloud intelligence identifies and visualizes sender domains and IP addresses.

EasySPF quickly and automatically builds error-free SPF records.

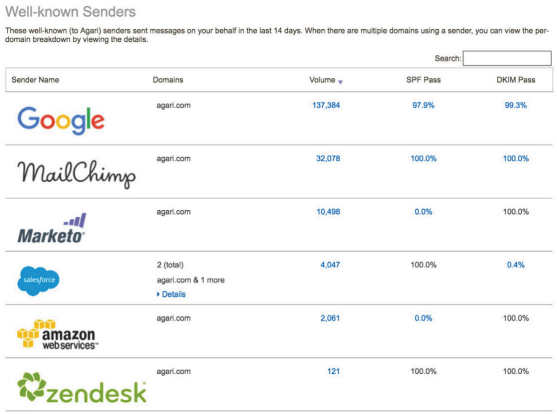
EasyDKIM automates selector identification and overall management of DKIM.

Data analytics give deep context on email domains including authentication, deliverability, abuse, and more.

Actionable Insight Into Your Email Ecosystem

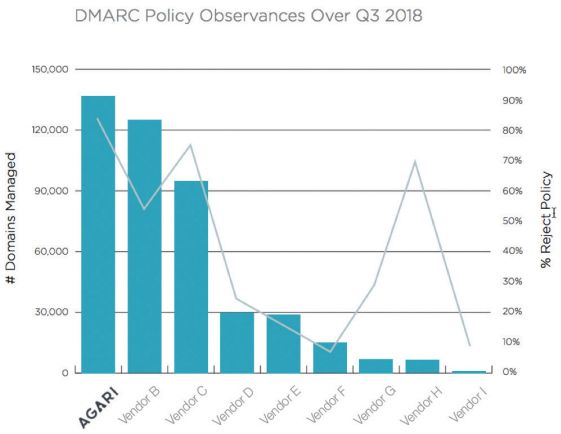
For many organizations, cloud-based email services such as Salesforce, Marketo, or Mailchimp represent the majority of emails sent to customers and partners. Often, organizations may not even know all the cloud service providers sending email on their behalf.

Agari Business Fraud Protection includes Email Cloud Intelligence, which automatically identifies, monitors, and manages emails being sent on your behalf by third-party email senders. This enables businesses to easily identify and authorize legitimate email communications, block malicious emails from cybercriminals and protect customers, partners, and employees from advanced email attacks including phishing and business email compromise.



Agari Business Fraud Protection In Action

Agari has a higher rate of enforcement than anyone and has helped more organizations realize business value by bringing their domains to a DMARC policy of Reject.



- Domains Protected: 132K+
- Domains with Reject Policy 81%

Agari Business Fraud Protection Deployment

Agari first works with you to understand your email environment by collecting and analyzing DMARC reports.

- » Protect your brand by instructing receiving mailboxes to reject all inbound messages that fail DMARC authentication.
- » Ensure authentication remains accurate as your email ecosystem changes.
- » Prevent look-alike domain attacks by continuously monitoring your ecosystem, even as cybercriminals switch to other attack types.

The Company We Keep

Top 3 Social Networks | 6 of the Top 10 Banks | Top Cloud Providers

Microsoft HSBC aetna facebook citi CHASE Google

Learn More: www.agari.com/products