appgate

Leverage Appgate Email Protection as a key component of a comprehensive anti-fraud program

Appgate Email Protection

Fraudulent messages and orchestrated attacks have eroded trust in email as a means of communication to such an extent that it is nearly impossible for major financial institutions, retailers, and merchants to reach their customers authentically. Fortunately, the draft DMARC specification, created by a group of leading email providers, shows great promise for protecting email channels, reducing the amount of spoofed email received, and improving threat intelligence and visibility around targeted attacks. This white paper explains the draft DMARC specification and how to leverage it to reduce phishing attacks and strengthen customer trust in their email communication.

What is Appgate Email Protection?

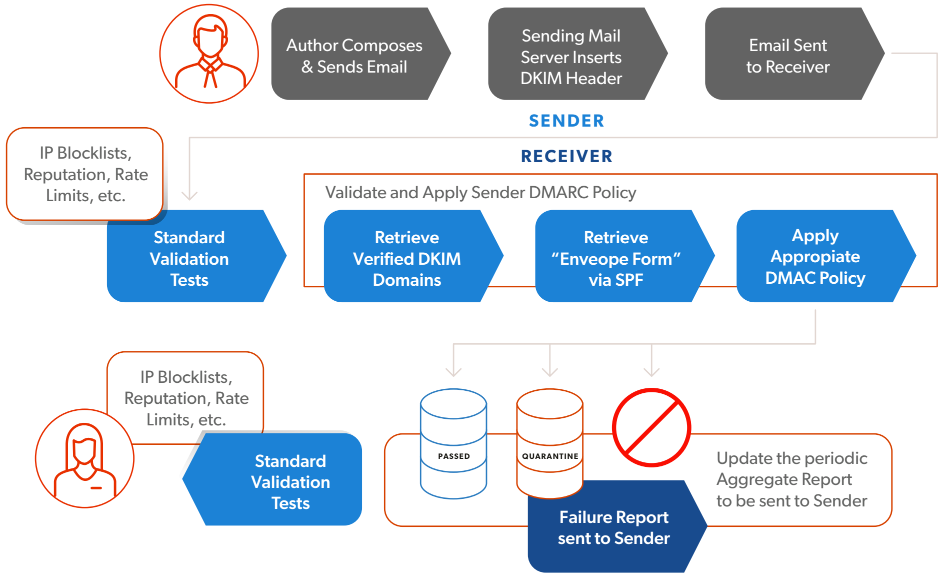
Our solution powered by **DMARC[1] "Domain-based Message Authentication, Reporting, and Conformance"**, **DMARC** is an e-mail authentication protocol that allows e-mail domain owners to specify what mechanisms they use to authenticate their e-mail messages and how mail servers that receive messages from their domain should handle authentication failures.

DMARC aims to help combat email fraud and phishing attacks by allowing email recipients to determine if an email message claiming to come from a specific domain is actually from that domain. It works by allowing domain owners to publish policies that tell receiving email servers how to handle messages that fail authentication checks.

How does DMARC work?

Our solution is powered so, what is the mode of operation of DMARC and how does it work? A message is sent from an authoritative server to the SPF record of the DMARC-compliant domain and/or to the DKIM signature, which are stored at the DNS level. If any of the checks pass, the message is delivered; if both fail, the message is rejected and returned as undeliverable (as it did not meet SPF or DKIM requirements).

Once you have successfully configured DMARC for your domain, you can enable reporting on which emails have been authenticated and which have not. This helps you identify suspicious messages so you can take action against them quickly and keep your subscribers safe.



Author Composes & Sends Email
Sending Mail Server Inserts DKIM Header
Email Sent to Receiver
SENDER
RECEIVER
IP Blocklists, Reputation, Rate Limits, etc.
Standard Validation Tests
Validate and Apply Sender DMARC Policy
Retrieve Verified DKIM Domains
Retrieve "Enveope Form" via SPF
Apply Appropiate DMAC Policy
IP Blocklists, Reputation, Rate Limits, etc.
Standard Validation Tests
PASSED
QUARANTINE
Update the periodic Aggregate Report to be sent to Sender
Failure Report sent to Sender

Why do we need Appgate Email Protection?

Spoofed emails enable the perpetration of phishing, malware, and spam. Established brands are often the lure used to fool unsuspecting customers. If a brand suffers numerous phishing attacks, its communications with customers will not be trusted. Brands must protect their businesses and customers with aggressive attempts to reduce spam, phishing and phishing that take advantage of their trademarks and name. Time and resources dedicated to brand awareness and engagement through email marketing can be undone in an instant with a massive and successful phishing incident; A recent survey found that 71% of U.S. adults with bank accounts would likely switch banks if they were victims of an online bank fraud attack at their current bank, to cite just one example. DMARC offers organizations a way to greatly reduce the chance of falling victim to such an attack.

WHAT ARE THE ADVANTAGES OF APPGATE EMAIL PROTECTION?

Here are some of the advantages of implementing Appgate Email Protection:

Prevents e-mail fraud:
You can prevent phishing attacks by using DMARC to identify fake emails and prevent them from reaching users' inboxes.

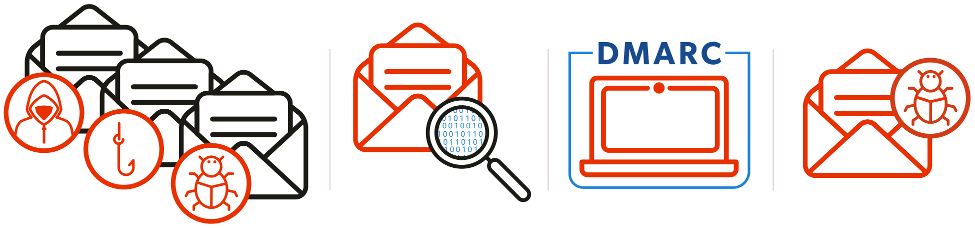
Improves brand reputation:
You can improve your brand reputation by making sure that only legitimate messages reach recipients' inboxes.

Minimizes spam:
You can reduce the amount of spam in your customers' inboxes by preventing fraudulent messages from reaching them in the first place.

Provides visibility:
Quickly identify who is sending emails on your behalf without your knowledge using DMARC reports.

Improves deliverability:
You can improve the deliverability rate of your email by 10% over time if you deploy the protocol correctly for your emails.

DMARC is important because previous efforts to verify that emails were authentic were not standardized and tended to attempt to authenticate in isolation from any other part of the email chain. Recipients made decisions about how to assess the authenticity of email on their own, and domain owners could never be sure whether recipients were receiving messages from imposters. DMARC solves this problem of many uncoordinated efforts to prove that emails are genuine by bringing them all together under one standard that all email senders and receivers are invited to use. A reliable way to distinguish real messages from fake ones is taking shape, which will make the email ecosystem a little more secure in the near future and potentially much more secure in the long term, improving the quality of email communication that is so needed. for businesses and their marketing teams to thrive.



DMARC solves this problem of many uncoordinated efforts to prove that emails are genuine by bringing them all together under one standard that all email senders and receivers are invited to use.

Any organization that trusts or sees value in a reliable email-based communication channel with its customers will benefit from implementing DMARC.

Some examples are illustrated in more detail below:

Financial Institutions

If your customers can't figure out which emails are from your financial institution and which are from phishers, this dilutes the customer's trust in your brand. This is not just an academic question. DMARC can ensure that the vast majority of fraudulent emails never reach unsuspecting customers in the first place.

Retails

Recent breaches at several prominent retailers, including Target, Neiman Marcus, and Home Depot, have shown vulnerabilities that exist at various points along the payment processing chain. But a breach is not the end of the harm suffered by retailers and their customers. The information stolen in these breaches is used to launch phishing attacks against the victim, often with the branding of the retailer where the breach occurred prominently displayed, offering help to mitigate the damage. But it's not just companies that have suffered a breach that could be affected. Fake emails that retail brands leverage offer discounts, promotions, coupons, promises of obscene content, and any other incentive they can think of to entice users to click on what is actually a phishing message. By the time the customer and retailer realize what has happened, cybercriminals have claimed another victim and the retailer's ability to engage customers via email has suffered. DMARC can maintain the reputation of retailers' brands and their customers by closing these types of emails before they reach an inbox.

Marketers

Have you ever wondered why your email marketing campaign doesn't seem to show any results? You've spent the money, collected the email addresses, and crafted a compelling message, but nothing seems to come out of it. Before DMARC, marketers had little idea of the level of risk they could be exposed to due to phishing or spoofed emails. But with all the data DMARC provides about email authentication, marketers can be more proactive in identifying and stopping attacks while making sure their legitimate messages are the ones their target customers actually open. Spam emails aren't even delivered, and the open rates of your email campaigns will increase as your customers click on fewer spoofed emails and become more confident in the emails your organization actually sends.

Bottom line: If you communicate with your customers via email, DMARC provides a clear path to being able to preserve the monopoly of emails being sent on behalf of your organization, so that trust crucial to effective communication is protected.

How to configure Appgate Email Protection?

Setting up DMARC can be a bit technical, but here are the general steps:

1. **Evaluate your email sending infrastructure:** Before configuring **DMARC** you must have a good understanding of your email sending infrastructure. This includes identifying all email servers and third-party services that send email on your behalf, such as marketing automation platforms, customer support tools, and email delivery services.
2. **Create a DMARC policy: A DMARC policy** tells e-mail recipients how to handle messages that fail DMARC checks. You must create a DMARC policy for each domain that you want to protect. The policy shall include the following elements:
   - **Policy mode:** You can choose between two policy modes: "none" and "quarantine" or "reject". "None" means that the receiver will continue to accept and deliver messages that fail DMARC checks. "Quarantine" or "reject" means that the receiver will send those messages to the spam or junk folder, or even reject them outright.
   - **Alignment requirements:** You can specify alignment requirements for your domain's SPF and DKIM records. This means that the domain name in the "From" header of an email must match the domain name in the SPF and/or DKIM record.
   - **Reports:** You can configure DMARC to send reports to your email address or to a third-party service. These reports will provide information about DMARC activity, including the number of emails sent, the number of emails that passed DMARC checks, and the number of emails that failed DMARC checks.
3. **Publish your DMARC record to your domain's DNS:** You can access your DNS management console to publish your record or ask your DNS hosting provider for help publishing it on your behalf.

DMARC records are published in the domain's DNS and are used by email recipients to determine the authenticity of emails sent from that domain.

What is a DMARC record?

A DMARC record is a Domain Name System (DNS) record that contains information about a domain's DMARC policy. specifies which e-mail authentication protocols (spf, dkim) the domain uses to verify incoming e-mail and what actions to take when an e-mail fails authentication checks, such as quarantining or rejection.

DMARC records are published in the domain's DNS and are used by email recipients to determine the authenticity of emails sent from that domain.

DMARC reports added to the email address specified by the domain owner on a periodic basis, summarizing the results of the DMARC evaluation of all emails received from that domain. These reports provide domain owners with useful information about the performance of their email authentication, such as how many emails were authenticated, how many DMARC checks failed, and which email providers send the most emails on their behalf.

When an email fails DMARC verification and is quarantined or rejected, email recipients send DMARC forensic reports. These reports provide more information about e-mail, such as the header and body of the message, as well as the IP addresses and host names of the sending and receiving mail servers. DMARC forensic reports are useful for troubleshooting DMARC problems and identifying potential sources of email abuse or fraud.

APPGATE EMAIL PROTECTION IN E-MAIL SECURITY

Appgate Email Protection and E-mail authentication

DMARC is a powerful email authentication protocol that helps protect domains from email fraud and abuse. Using DMARC, domain owners can specify which email authentication protocols (such as SPF and DKIM) to use when authenticating incoming e-mail and what action to take when an e-mail fails authentication checks.

Appgate Email Protection and domain spoofing

DMARC is an essential tool for protecting domains from phishing attacks, which are a type of email-based fraud in which an attacker sends emails that appear to come from a trusted domain. Spoofing attacks can be used for various malicious purposes, such as stealing sensitive information or distributing malware. DMARC helps prevent domain spoofing by authenticating emails sent from your own domain.

Appgate Email Protection and Phishing Protection

DMARC is a powerful tool in the fight against phishing attacks, which are a type of email-based scam that attempts to trick users into divulging sensitive information or taking malicious actions. By authenticating incoming email using DMARC policies, domain owners can protect their customers from phishing attempts by ensuring that only legitimate email reaches users' inboxes.

Appgate Email Protection and spam prevention

DMARC plays a crucial role in preventing spam messages from reaching users' inboxes. By authenticating incoming emails using DMARC policies, domain owners can help email providers distinguish legitimate emails from fraudulent ones, such as phishing attempts.

Take Your Brand Recall to the Next Level

Brand Indicators for Message Identification, or BIMI, is a standard that uses your brand presence to give your email more credibility. By affixing the logo of your brand on the emails you send, it acts as a second level of verification to let your customers know it's genuine.

Appgate Email Protection & Digital Threat Protection

The powerful combination of Appgate Email Authentication and Digital Threat Protection (DTP) fraud monitoring solution, goes several steps further than any other DMARC vendor, stopping a wider range of attacks. Other DMARC solutions provide reports, but DTP gives you the ability to gain intelligence from those reports and use them to shut down attacks. Essentially, DMARC limits the attacks delivered and DTP cleans those that still manage to sneak in. DMARC with DTP provides complete visibility into email flows, with real-time attack monitoring, reporting, and elimination of active attacks, something other DMARC solutions are not equipped to offer. Unifying DMARC compliance with DTP's proactive threat intelligence gives your organization a truly comprehensive way to combat fraud against your brand.

WHY DO YOU NEED BIMI?

These are the best things about BIMI:

Brand Recall: Every time you send an email, your customers will see your logo in their inbox, reinforcing your brand image.

Customer Confidence: A familiar logo will be recognisable to customers as a brand they have a relationship with.

Email Deliverability: An email that's immediately identified as trust-worthy is much more likely to reach inboxes and get clicks.

Visual Confirmation: Your logo is verified along with your email, so it's an easy way to indicate your message has been authenticated.

DMARC-Based: BIMI builds on a foundation of DMARC, giving you more security with your existing DMARC deployment.

About Appgate

Appgate is the secure access company. We empower how people work and connect by providing solutions purpose-built on Zero Trust security principles. This people-defined security approach enables fast, simple and secure connections from any device and location to workloads across any IT infrastructure in cloud, on-premises and hybrid environments. Learn more at appgate.com

[1] Appgate Email Authentication is powered by Power DMARC

appgate