ValiMail

An Insider's Guide To Email Authentication Through DMARC

180 Montgomery St., 18th Floor
San Francisco, CA 94104

info@valimail.com
www.valimail.com

What Is Email Authentication and Why Do I Need It?

Email is the primary communications medium globally, with over 6.3 billion mailboxes used by 3.7 billion people worldwide in 2017 — half the planet — and it continues to grow. (Radicati 2017) 98.5% of Internet users check email daily, and the average U.S. white collar worker spends 6.3 hours a day checking email — even in the bathroom. (Adobe 2015)

However, email is vulnerable: Without authentication, it is impossible to be sure that the sender of a message really is who they appear to be. This lies at the root of the recent explosion of email-based fraud. Just a few data points:

EXPLOSION OF EMAIL-BASED FRAUD

$11.7 MILLION	What the average company spends dealing with cybercrime each year (Accenture 2017)
90%	Proportion of all hacks and cyber attacks that start with email messages (Verizon DBIR 2017)
77%	Average reduction in email threats after implementing email authentication (GreatHorn 2017)
$5.3 BILLION	Total cost of business email compromise (BEC) attacks (FBI 2017)

These attacks damage the brand being impersonated, lead people to trust their emails less, and can potentially open a company up to further hacks, ransoms, lawsuits, and other costs.

What's more, legitimate emails that aren't authenticated may be marked as suspicious by receivers and may even be quarantined or rejected, hurting overall deliverability.

This is a particular problem for enterprises using cloud services. For a typical organization there may be 20 or more such services, including their payroll provider, benefits manager, digital marketing company, customer support agency, legal discovery services, and more. Often, the IT department is unaware of these "shadow email" senders.

Worldwide Email User Forecast, 2017–2021

Year	2017	2018	2019	2020	2021
Worldwide Email Users (M)	3,718	3,823	3,930	4,037	4,147
% Growth	~	3%	3%	3%	3%

Source: Radicati

DMARC Adoption Is Growing Exponentially

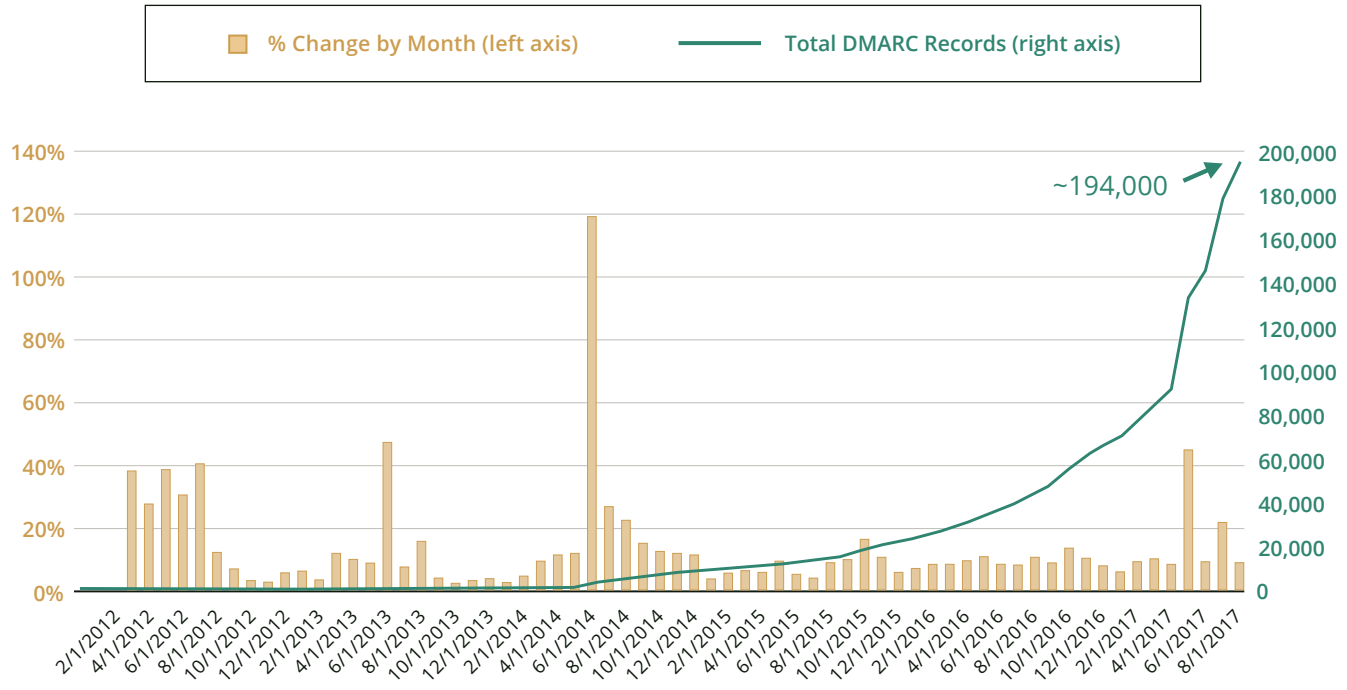
DMARC (Domain-based Message Authentication, Reporting and Conformance) is a widely-accepted open standard that ensures only authorized senders can use your domain in the From: field of their email messages. It incorporates and builds upon two earlier email authentication standards, SPF and DKIM, and used together these three technologies can prevent important classes of email phishing attacks.

For DMARC to work, the sending domain needs a DMARC record and the receiving server needs to check for that record and see if the sender is authorized. DMARC records are stored as text records in the Domain Name System (DNS).

Fortunately, 4.6 billion email inboxes worldwide now accept the DMARC standard, including all of those from major email services providers such as Google, Microsoft, Yahoo, and AOL. Overall, 76 percent of the world's inboxes will enforce a DMARC policy, if the domain owner has published one.

On the sending side, DMARC adoption is growing exponentially. Over 60,000 domains now publish a DMARC record, protecting those domains from phishing and email impersonation.

Growth of DMARC Adoption Globally



Source: 2017 Trusted Domain Project
Data provided by Farsight Security Graph

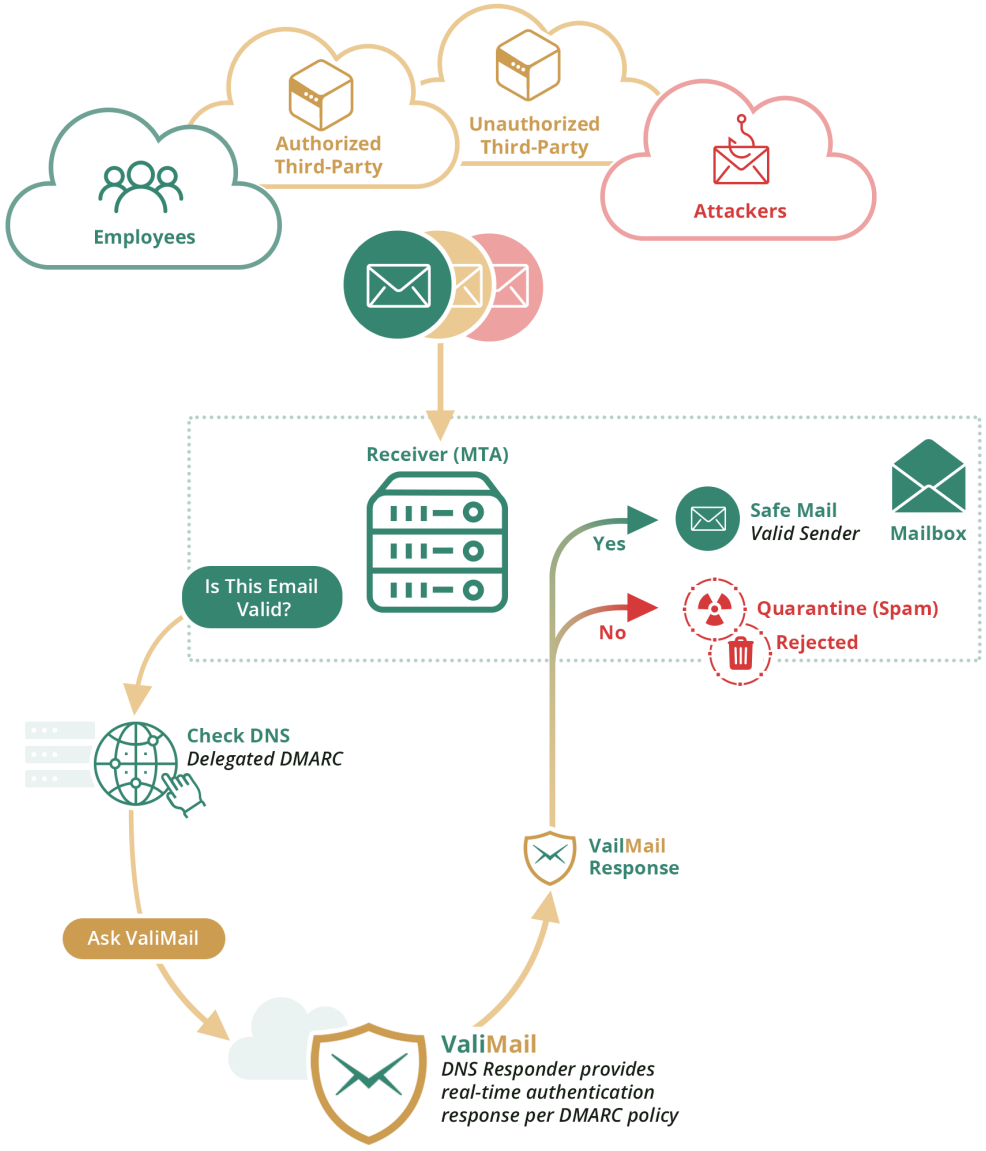
How DMARC Defends Against Exact-Domain Phishing

Receiving mail gateways that follow the DMARC standard examine each incoming email message to determine whether the sender is authorized to use the domain listed in the From: and Reply-to: fields.

If there is a DMARC record and the email fails the tests, the receiving mail server follows the instructions shown in that record to determine what to do with the email: Reject it, quarantine it (by putting it in a spam folder), or do nothing. It also sends a log of what was done back to the domain owner.

Note that rejected emails never even get to the recipient's inbox: They are rejected outright by the receiving email server.

If there is no DMARC record, some email service providers, including Google and Microsoft, have started showing a warning to the end user, such as a question mark indicating the sender's identity can't be confirmed.



DMARC for Monitoring, Shadow Email Discovery, and Deliverability

DMARC provides many benefits to enterprise IT. The first is inbound protection for the enterprise. DMARC at enforcement prevents email impersonation that can enable phishing or business email compromise (BEC). DMARC also provides outbound protection, preventing an organization's name from being hijacked by scammers in phishing attempts aimed at customers or partners.

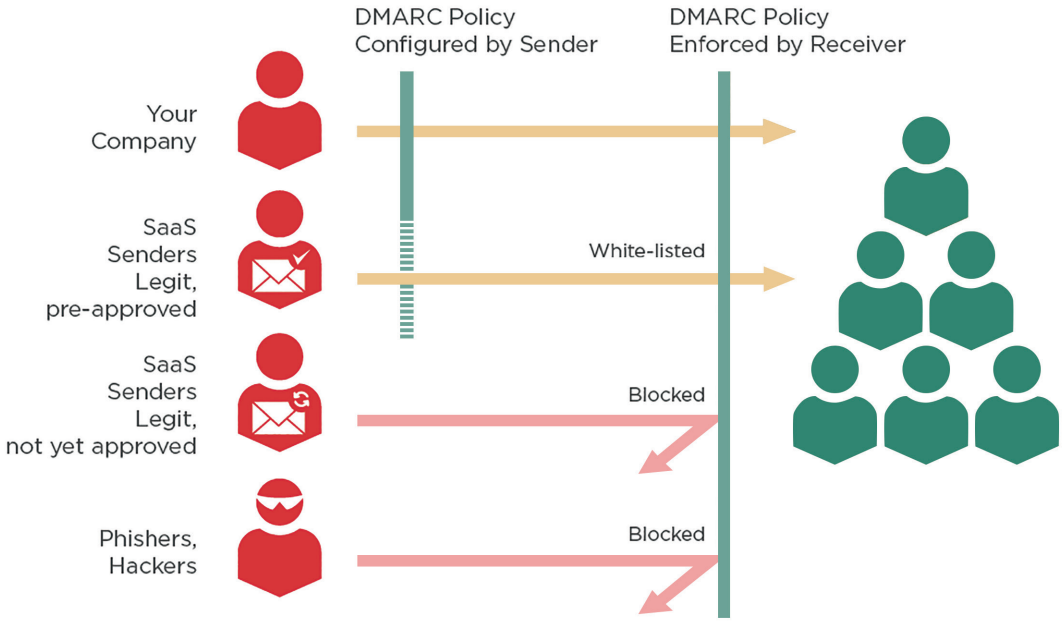
Once an organization sets up a DMARC record, no sender will be able to deliver email on behalf of the organization without getting on the DMARC whitelist.

Additionally, because of DMARC's reporting features, your IT team will be alerted to any services that are attempting to send mail using the domain, enabling them to determine whether those services are legitimate or not. In this way, DMARC gives IT a powerful tool for discovering and authorizing "shadow email" cloud services.

What's more, DMARC in enforcement mode prevents all same-domain phishing attacks and BEC attacks.

Finally, publishing DMARC records is increasingly important to ensure emails are delivered, unaltered and unflagged, to intended receivers. If there is no DMARC record for a domain, some email service providers may warn the end user, and some may not even deliver the message, or send it to a spam folder. That increases the urgency for organizations to implement email authentication so their legitimate emails don't get flagged as suspicious.

DMARC Policies Tell Receivers How to Authenticate Email from Your Domain



The DMARC Implementation Challenge

Despite DMARC's enormous advantages, ValiMail has found that 77 percent of organizations that attempt to implement it aren't getting it right, for a variety of reasons.

- DNS updates are subject to internal controls and delays in many organizations.
- SPF, DKIM and DMARC records contain long strings of text and numbers and are easy to get wrong. A single typo renders them invalid, often without no indication until long after users' email stops getting delivered.
- DMARC reports sent by receiving email servers are complex and difficult to parse: How do you know if 209.177.162.31 should be sending emails on your behalf?
- DNS records must be updated continuously as new sending services are authorized (and de-authorized), sending services change their email servers, and keys are updated.

ValiMail examined over 1 million of the world's highest-traffic domains. We found that, of those that have published DMARC records, the vast majority either had configuration errors or hadn't set it to enforce the whitelist. Even large enterprises with big IT departments have approximately the same failure rate as smaller sites.

In short: It's not easy to get it right.

Failure Rate
(of those attempting authentication)

NASDAQ 100	72.1%
FTSE 100	80.0%
S&P 500	74.4%
Fortune 500	82.4%
Crunchbase Unicorns	60.2%
.Gov Domains	79.0%
Majestic Million	76.7%

All organizations, large to small, have similar failure rates.

DMARC in Detail

Email services authenticate received messages by doing a series of checks using information published in the global DNS system. A domain owner can publish three types of records in DNS for their domain:

SPF

A whitelist of IP addresses for authorized senders

DKIM

A public key for validating a digital signature generated by the authorized sender and sent with the message

DMARC

A set of policies that tells receivers what to do with messages that fail authentication and where to send reports

For each message, the receiving server can check the SPF record to determine if the message came from an approved server's IP address. It can also use the key in the DKIM record to validate that the sender is allowed to send email from the domain shown in the message's "from" and "reply to" addresses. If either of these checks fail, the DMARC record tells the receiver what to do: Reject the message, quarantine it in a spam folder, or make its own, local decision.

Additionally, DMARC requires the SPF and DKIM addresses to be "aligned" with the human-readable From address — an important step if you're going to prevent fraud.

One complication is that SPF allows senders to list authorized servers by IP address or by domain name — but it will only check the first 10 domains listed. Since each cloud service can easily require 3-4 lookups, you can hit the 10 lookup limit with as few as 3 services.

If you list mail servers by IP address, you will need to update that list whenever those servers' IPs change — a maintenance nightmare.

Can you identify the bad record?

```
_dmarc.example.com
v=DMARC1; p=none; fo=1;
rua=mailto:reports@rua.example.com,
mailto:dmarc_agg@dmarc.example.com;
ruf=mailto:reports@ruf.example.com,
mailto:dmarc@dmarc.example.com;
```

```
_dmarc.example.com
v=DMARC1; p=none; fo=1;
rua=mailto:reports@rua.example.com,
mailto:dmarc_agg@dmarc.example.com;
ruf=mailto:reports@ruf.example.com,
mailtodmarc@dmarc.example.com;
```

Spot the mistake

Automation is the Key to Successful Email Authentication

Email authentication is extremely powerful, but it requires careful configuration of DNS, intimate knowledge of the email infrastructure of thousands of sending services, constant monitoring, and rapid updating to respond to attacks and to changes in cloud services. Monitoring tools can help, and consulting services can provide guidance, but a pretty GUI and good advice simply won't get it done for most companies. Implementing email authentication successfully requires a fully automated approach that eliminates the need for mapping the Internet's email servers, interpreting DMARC reports, and touching DNS with every update.

ValiMail offers a turnkey "email authentication as a service" product. Our automated service replaces manual effort and guesswork with automation and intelligence, bringing the benefits of email authentication to any size organization. Here are some of the features:

- Fixes built-in standards limitations
- Auto-detects & classifies email-sending services
- Authorizes/de-authorizes senders with one click
- Eliminates iterative & manual DNS changes
- Flags malicious activity in real time
- Organizes DMARC log data into easy-to-read reports

For more information on ValiMail's email authentication cloud, contact us at **info@valimail.com**.

About ValiMail

ValiMail has developed the world's first cloud service that fully automates email authentication, giving our customers both inbound and outbound brand and fraud protection across 4.8 billion mailboxes worldwide. ValiMail enables organizations to stop phishing attacks, control shadow email, and improve the reputation of their email domain. ValiMail's patented, standards-compliant technology provides the only zero-administration solution to enable trusted email for enterprises. Customers include Uber, Fannie Mae, Yelp, Twilio, Time Warner, OpenTable, and City National Bank. Founded in 2015, ValiMail is based in San Francisco and is backed by Shasta Ventures, Flybridge Capital Partners, and Bloomberg Beta. For more information visit **www.valimail.com**.