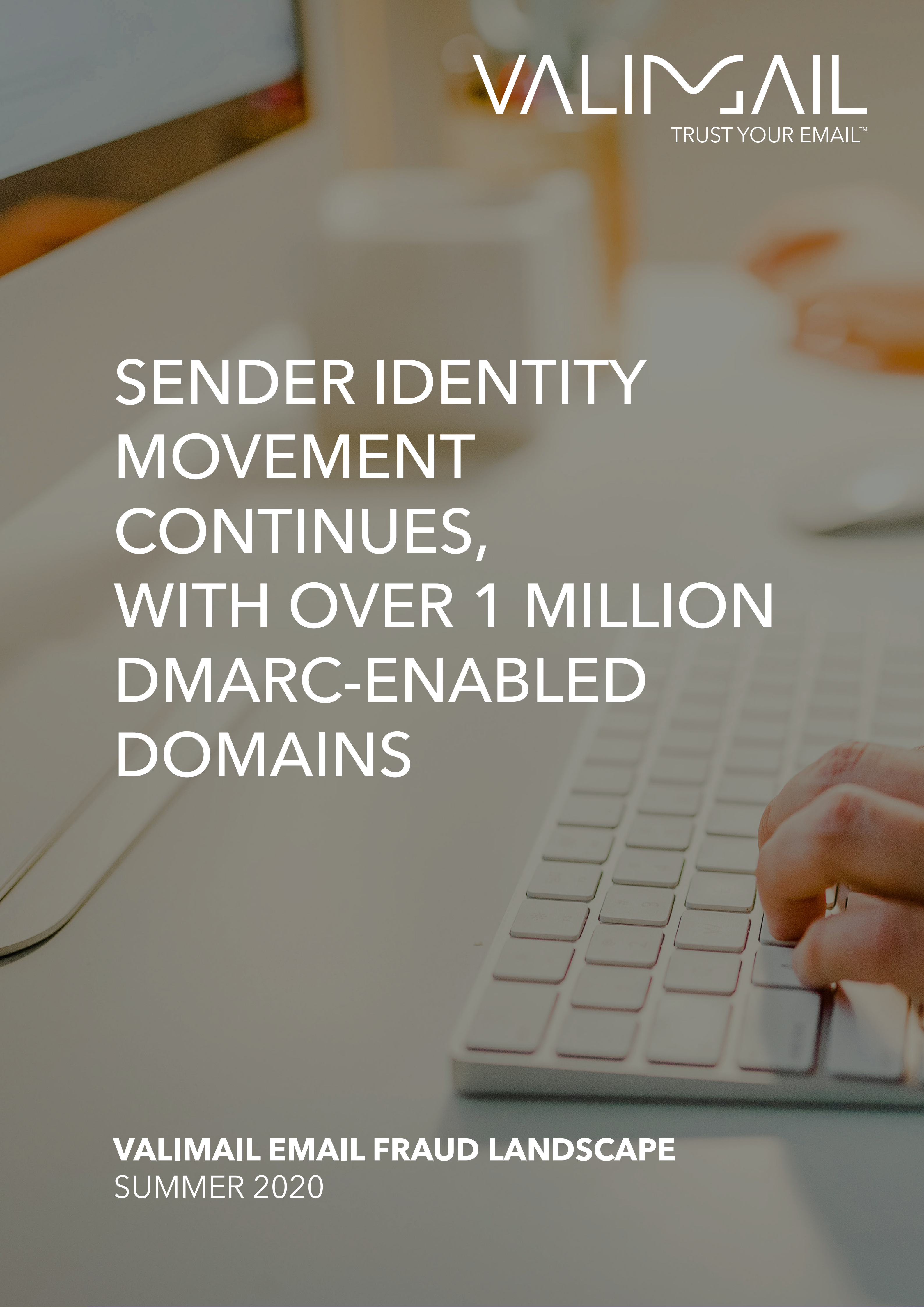


VALIMAIL
TRUST YOUR EMAIL™

SENDER IDENTITY MOVEMENT CONTINUES, WITH OVER 1 MILLION DMARC-ENABLED DOMAINS

VALIMAIL EMAIL FRAUD LANDSCAPE
SUMMER 2020

INTRODUCTION

Valimail has been tracking the usage of Domain-based Message Authentication, Receiving, and Conformance (DMARC) across tens of millions of domains since early 2017. During that time, we've seen consistent growth in DMARC usage and its overall effectiveness.

Now, for the first time, the number of domains with DMARC records exceeds one million. This is a significant milestone.

Valimail's analysis is based on DNS inspection of tens of millions of domains from publicly traded and privately held for-profit companies, nonprofits, governments, as well as NGOs. It also includes the 1 million domains with the highest traffic, as well as many other sources of organizational domains. While there are many more domains in existence (almost 360 million, according to one estimate), hundreds of millions of domains are either unused or are being utilized by spammers, phishers, and hackers for deception campaigns. Many of these phishing domains also utilize DMARC, but are not included in Valimail's analysis.

Our study is limited to domains for which we can attribute, with reasonable confidence, the existence of a real-world organization or entity of some kind. As a result, we believe that the numbers in the following pages are the most accurate and representative picture of DMARC adoption among legitimate organizations and domain owners.

BACKGROUND

Impersonation is the engine that drives the #1 cybersecurity attack vector: Phishing. Phishing attacks of just one type — business email compromise (BEC) — have caused at least $26 billion in losses in the past five years, according to the FBI. Other sources have noted that 83% of email attacks are brand impersonations and another 6% are impersonations of people, meaning nearly 90% of all email attacks rely on deceptive sender identity.

A variety of solutions have been introduced to stop the onslaught of phishing, including artificial intelligence-based behavioral analysis, block lists to screen out known phishing domains, and complex rulesets aimed at eliminating imposters.

KEY FINDINGS

1 million+ domains now use DMARC

13.9% overall enforcement effectiveness

30% enforcement rate among Fortune 500 DMARC records

79% of Fortune 500 domains can still be spoofed, because they either have no DMARC, or they are using DMARC in "monitor mode"

75% of U.S. federal domains are protected from spoofing by DMARC enforcement

DMARC usage and enforcement are growing, and are increasingly recommended or mandated by many organizations and governments

> "83% of email attacks are brand impersonations and another 6% are impersonations of people, meaning nearly 90% of all email attacks rely on deceptive sender identity."

But one of the most effective components of an integrated email defense is DMARC. DMARC addresses the core technique used by most phishers: Domain spoofing (i.e. using the exact domain of the entity they're spoofing in the From field of the phishing message). It gives domain owners visibility into what services (and which bad actors) are sending email "from" their domains. When configured properly, with an enforcement policy, it prevents spoofing of those domains by unauthorized senders. Once at enforcement, a domain can only be used by authorized senders. Email attackers are then forced to rely on other, easier-to-detect impersonation techniques — or they move on to other targets.

In short, DMARC is a key component of an identity-based, zero-trust email security strategy: One in which only authorized senders are allowed access to the domain.

As we uncovered in our last research report, the number of attempts to spoof a domain typically drops to zero or near zero within a few months after that domain moves to DMARC enforcement, as would-be impersonators give up and move on to other targets or adopt other techniques.

One the receiving side, major email receivers have been supporting the standard for years. Valimail data has shown for several years that about 80% of the world's inboxes (including virtually all U.S.-based email providers) do DMARC checks on inbound email messages, enforcing the domain owner's stated policies.

GROWTH OF DMARC USAGE AND ENFORCEMENT

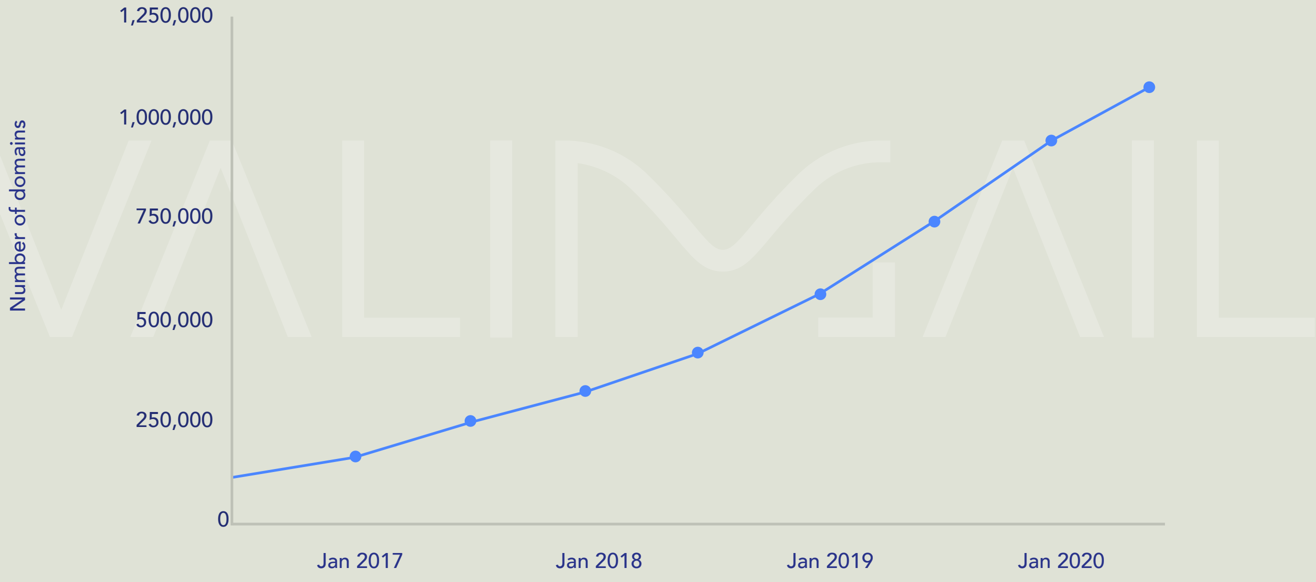
On the sending side, more and more domain owners are waking up to DMARC's potential. As of June 1, 2020, 1.07 million domains have published DMARC records.

That's an increase of 48% over one year prior, and almost 2.5X the number of DMARC records over two years ago.

Of these 1.07 million DMARC records, 148,300 (13.9% of the total) have enforcement policies (p=reject or p=quarantine, with 100% coverage and no exceptions for subdomains).

Many organizations have called on companies and governments to enforce DMARC policies. In 2017, the U.S. Department of Homeland Security mandated it for all non-military,

TOTAL DOMAINS WITH DMARC



NOTE: VALIMAIL'S ANALYSIS COUNTS ORGANIZATIONAL DOMAINS ONLY. WE ARE NOT INCLUDING SUBDOMAINS IN THESE TOTALS. SOURCE: VALIMAIL non-intelligence domains within the executive branch (see Binding Operational Directive 18-01). The U.S. Federal Trade Commission has also encouraged companies to use DMARC enforcement. More recently, in June 2020, the industry group M3AAWG issued a recommendation, in response to the surge of COVID-19 related phishing attacks, that all organizations should move to use DMARC enforcement.

But if only 13.9% of all domains that deploy DMARC are actually enforcing it, does that mean that these calls to action have failed? Far from it.

Among large enterprises, we see a much higher rate of enforcement — and these rates are rising. For instance:

- Among Fortune 500 domains, 30% of the DMARC records are at enforcement, up from 23% a year ago.
- Among large banks, 36% of DMARC records have enforcement, up from 29% a year ago.
- And in the U.S. federal government, 92% of DMARC records are at enforcement, thanks to the DHS order mentioned above.

In short, enterprises, both commercial and government, are starting to get the message: For DMARC to be effective, you need an enforcement policy.

Of course, there is still much room for improvement. Too many organizations find it difficult to reach DMARC enforcement due to the complexity of their email ecosystems and the fear of accidentally blocking good senders when moving to a more restrictive policy. If you don't get all the authorizations in SPF and DKIM exactly right, a DMARC enforcement policy could unintentionally prevent legitimate emails from being delivered. For this reason, many organizations deploy DMARC, but then stall at the "monitor" phase (p=none) as they get overwhelmed with the complexity and tedium of the project.

PROTECTED BY DMARC WITH ENFORCEMENT

	Protection Rate
Billion-dollar public companies	14%
Global banks and financial services	21%
Fortune 500	21%
Global media companies	10%
Global technology	19%
U.S. federal government	73%
U.S. health care	11%
U.S. utilities	8%

SOURCE: VALIMAIL

DMARC DEPLOYMENT BY INDUSTRY

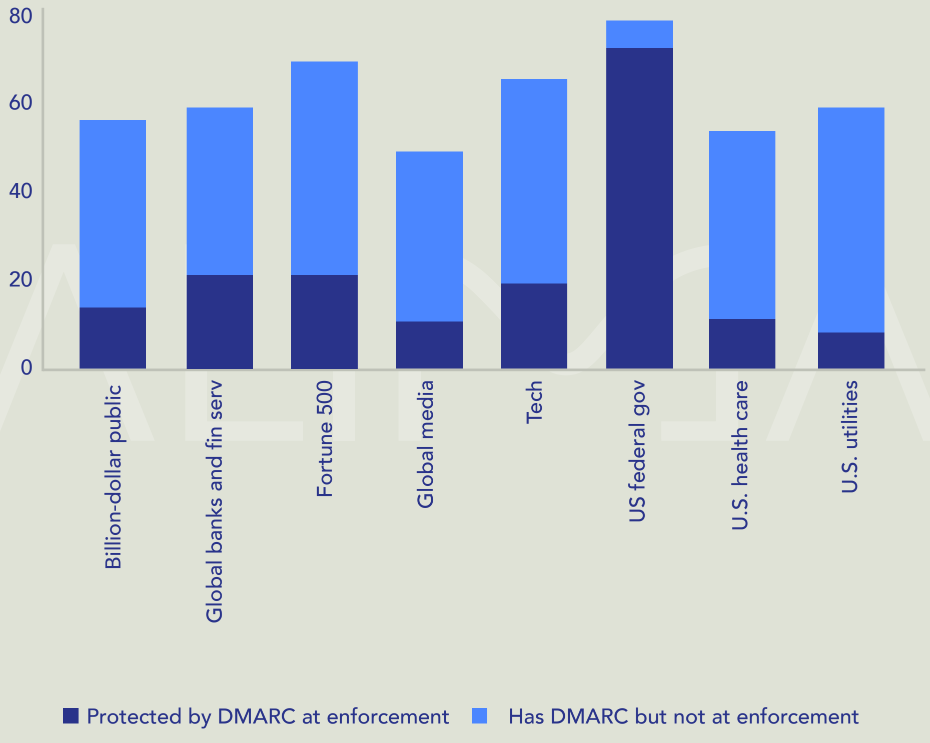
For this report, as for previous reports, Valimail analyzed the DMARC status of eight different industry cohorts. In nearly every category, we limited the analysis to companies with $1 billion or more in annual revenues, and focused on each organization’s primary domains. For media companies we used a lower revenue cutoff of $500 million annually, and for federal government domains there was no revenue limit — we included all U.S. federal government domains as tracked by Data.gov. The Fortune 500 includes all 500 companies in that list.

As in previous reports, the federal government is far and away the leader, with 73% of domains protected by DMARC. The closest any private sector industries got to that enviable benchmark was 21%, with global banks and Fortune 500 companies tied for the honor of second place. Tech companies came in third at 19% protected, perhaps surprisingly given this sector’s natural affinity for technical solutions and Internet standards.

In the below chart, you can see the relative proportions of domains with and without enforcement for each category. The total height of each column shows what percentage of that industry category has DMARC records; the lighter section of each column represents DMARC records in “monitor mode,” and the darker, lower section represents DMARC records at enforcement.

In other words, a high rate of DMARC deployment — as with Fortune 500 and U.S. utility companies — doesn’t necessarily translate into a high level of protection, unless it’s also paired with a good enforcement rate.

DMARC STATUS BY CATEGORY



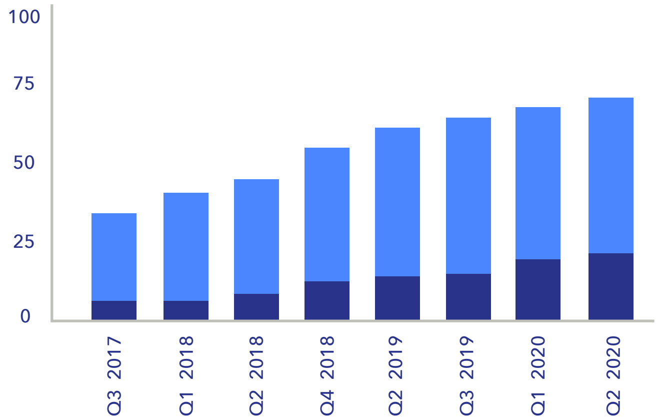
SOURCE: VALIMAIL

SELECTED INDUSTRY SNAPSHOTS

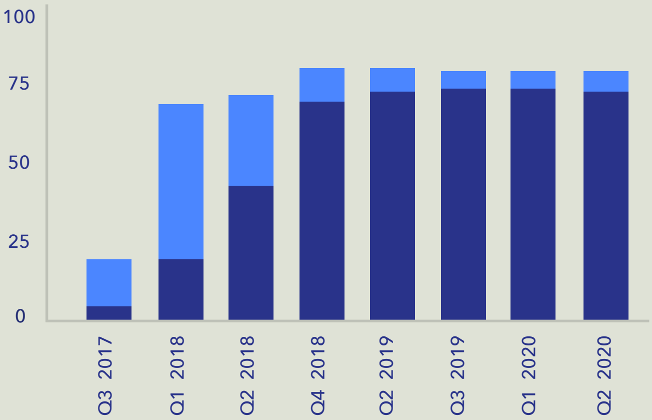
You can see how certain categories have progressed over the years in both dimensions: DMARC deployment, and enforcement effectiveness.

In the Fortune 500, DMARC deployment has steadily increased, from 34% in Q3 2017 to 70% today. Meanwhile, enforcement effectiveness has increased somewhat, with the result that 21% of Fortune 500 companies' primary domains are now protected from being spoofed.

FORTUNE 500



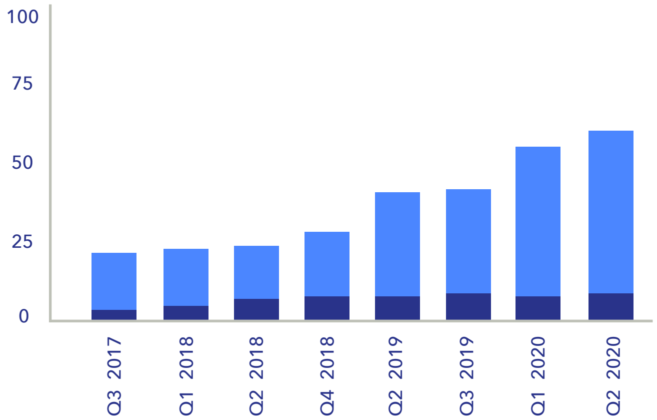
U.S. FEDERAL GOVERNMENT



In the federal government, we saw a sharp spike in DMARC record deployment in Q2 2018, as agencies began to respond to the DHS order, BOD 18-01, and began publishing DMARC records. At first, most of those records were in monitor mode, but over the subsequent two quarters we saw a rapid increase in enforcement effectiveness, as the majority of domains moved into compliance with the order. At present, the remaining domains that lack DMARC are mostly those unaffected by BOD 18-01 (military, intelligence, and judicial branch domains).

Among utilities, we've seen a steady upward trend in the number of domains deploying DMARC, and 60% of utility domains now have DMARC records. However, because enforcement rates remain low, utilities are still largely unprotected from domain spoofing: Only 8% of all utilities have achieved DMARC enforcement.

U.S. UTILITIES



■ Protected by DMARC at enforcement ■ Has DMARC but not at enforcement

SOURCE: VALIMAIL

"The time to deploy DMARC is now – and your deployment plan should include a path to enforcement."

TAKEAWAYS FOR DOMAIN OWNERS

DMARC deployment, and DMARC enforcement, are gaining momentum. The standard is no longer limited to "early adopters" or companies on the cutting edge of email technologies. It's supported by 80% of email inboxes worldwide, meaning those inboxes will respect the allow lists and rules you set, and reject or quarantine (send to a spam folder) unauthorized email from your domain, if you have configured DMARC with an enforcement policy.

What's more, DMARC is widely recommended by a variety of government agencies and industry organizations, it's effective at curbing one of the most pernicious forms of phishing, and it helps organizations gain better control over the many email senders that they use.

In other words, the time to deploy DMARC is now — and your deployment plan should include a path to enforcement.

In order to get to enforcement without accidentally causing good mail to get blocked, you'll need visibility. Fortunately, DMARC includes provision for exactly that, because built in to the standard are requirements that mail gateways send DMARC reports to domain owners, specifying (in aggregate) the senders that passed authentication and those that failed. Most mail gateways do this, including all the big, commercial providers of consumer email services, such as Yahoo Mail and Gmail.

With a good DMARC monitoring and analysis tool, you can turn those DMARC reports into actionable insights that let you know exactly what services need to be allowed, what the impact on your mail deliverability is, and how to get those services to authenticate properly.

TAKE THE FIRST STEP TO DMARC ENFORCEMENT

Valimail offers a DMARC visibility tool called Valimail DMARC Monitor™, and it's free to use.

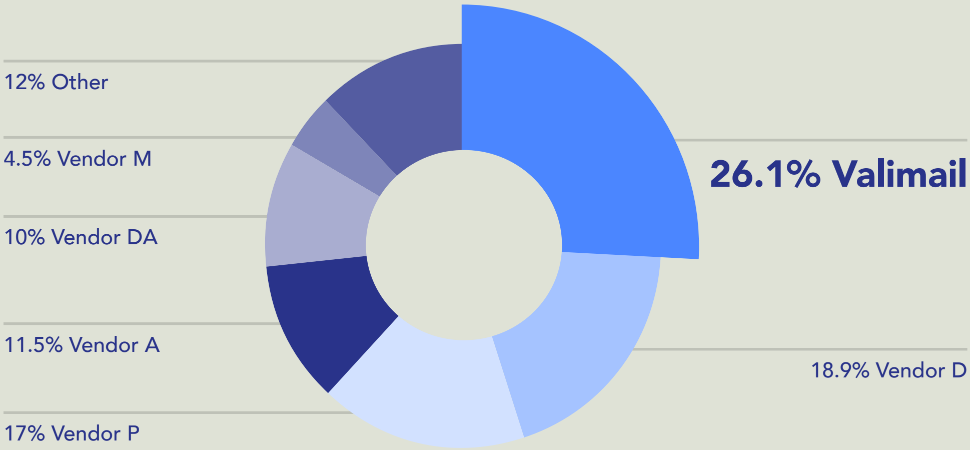
DMARC Monitor provides the simplest, most effective, most accurate way to reveal all the services sending from your domains – including senders spoofing your identity to phish your employees, partners, customers and everyone you do business with.

DMARC Monitor turns DMARC reports into easy-to-read lists of services, giving you visibility into all the services sending email "from" your domain, including those that are mostly passing authentication, partially passing, or mostly failing – even if those services only send a handful of messages a month.

The better visibility you have, the quicker and easier it is for you to take steps towards stopping brand abuse and email spoofing. DMARC Monitor provides the best, most complete visibility in the market.

Find out why more companies use Valimail than any other DMARC solution in the market, and why Valimail customers have the highest rate of DMARC enforcement in the industry. ▸

DOMAINS WITH DMARC ENFORCEMENT



TRUST YOUR EMAIL

Valimail is the global leader in zero-trust email security. The company's full line of cloud-native solutions authenticate sender identity to stop phishing, protect brands, and ensure compliance; they are used by organizations ranging from neighborhood shops to some of the world's largest organizations, including Uber, Splunk, Yelp, Fannie Mae, Mercedes Benz USA, and the U.S. Federal Aviation Administration. Valimail is the fastest growing DMARC solution, with the most domains at DMARC enforcement, and is the premier DMARC partner for Microsoft 365 environments. For more information visit www.valimail.com.