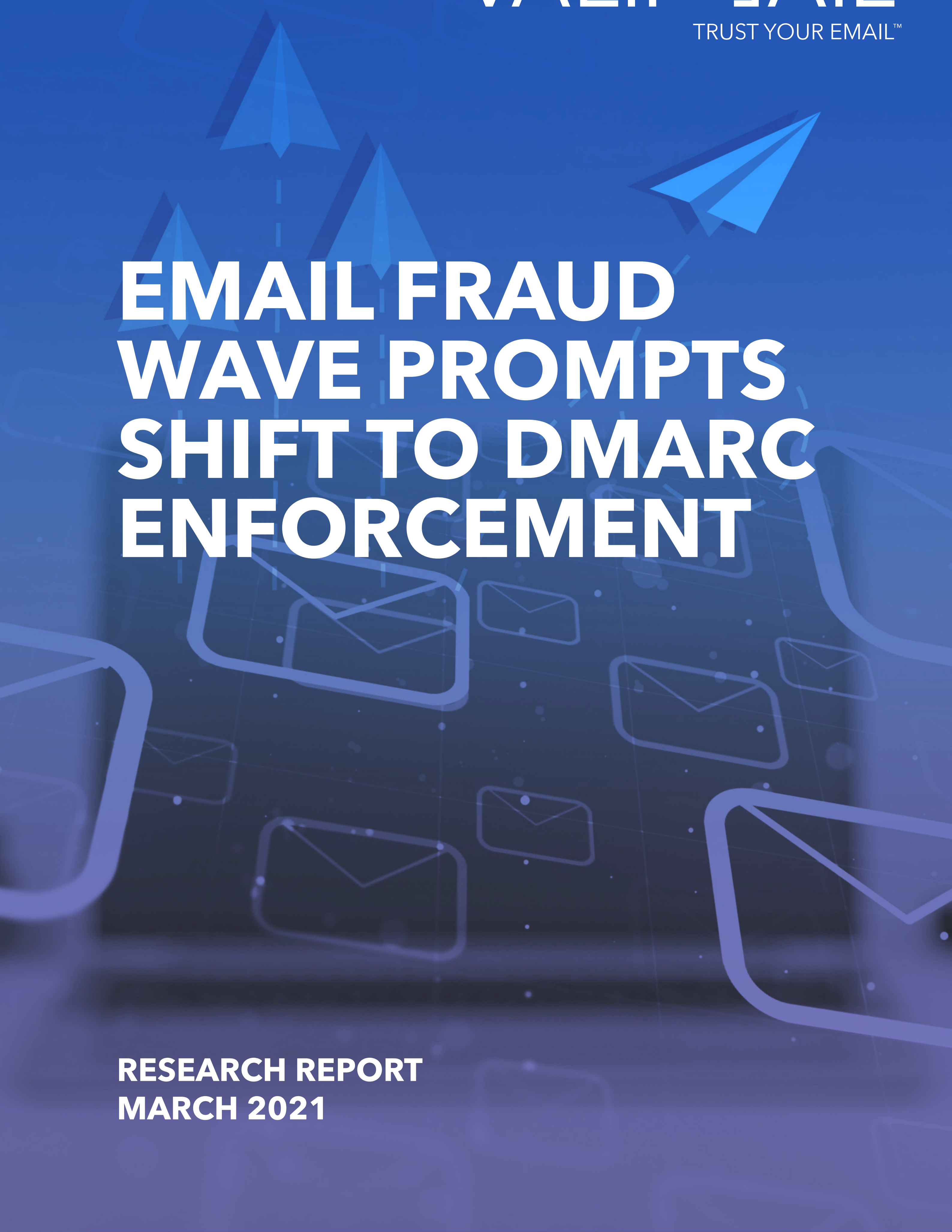
VALIMAIL
TRUST YOUR EMAIL™



EMAIL FRAUD WAVE PROMPTS SHIFT TO DMARC ENFORCEMENT

RESEARCH REPORT
MARCH 2021

BACKGROUND

Email continues to be one of the most effective ways to communicate. This accounts for its growth during a year of global pandemic, but also for the fact that hackers continue to use email as a primary attack vector.

Four billion human beings rely on email, according to the most recent Radicati Group estimates. That's a bit more than half the planet's population — and the rate of email usage continues to grow, adding users at a rate of 3% per year. Radicati notes that "email remains a key component of the online experience," forming the common denominator (and underlying notification medium) for social networking sites, chat apps, instant messaging services, shopping sites, and more. The firm estimates that worldwide email traffic exceeds 300 billion emails per day as of late 2020.

With many people quarantined or on partial lockdowns and ordinary business disrupted throughout much of 2020, businesses have redoubled their efforts to use email in order to stay connected with customers. According to a recent Sparkpost survey, 44% of marketing leaders increased their email marketing budgets in 2020, and 60% agreed that email is a primary source of revenue for their organizations.

Yet email continues to be a leading vector for cybercrime, implicated in over 90% of all cyberattacks. And the pandemic has provided a new leverage point for these attacks. Since the beginning of COVID-19, email security providers (ESPs) reported a surge in pandemic-themed phishing attacks. These scams took advantage of people adjusting to working from home, in environments where they're easily distracted, with less-secure computer hardware and networks.

Indeed, phishers continue to readily deploy attacks, with the average phishing campaign lasting a mere 12 minutes, according to Google, which has stated that it blocks over 100 million phishing emails per day, and that 68% of them are new, never-before-seen scams. And, according to research by Barracuda, 89% of all email attacks utilize impersonation, primarily of trusted brands (83%) but also of individuals (6%).

AT A GLANCE

At least 1% of global email traffic utilizes suspicious and likely fraudulent sender identity

That means 3 billion messages per day are spoofing the sender identity used in their "From" fields

Domains without DMARC enforcement are 4.75x more likely to be the target of spoofing attempts than domains with DMARC enforcement.

80% of all email inbox providers do DMARC checks on inbound email

More than 1.28 million domain owners worldwide have configured DMARC for their domains

Overall, only 14% of domains with DMARC are actually protected from spoofing by an enforcement policy

But DMARC enforcement is growing: Among large organizations, 43.4% of domains with DMARC are using enforcement

The U.S. federal government leads with DMARC usage, with 74% of all domains protected

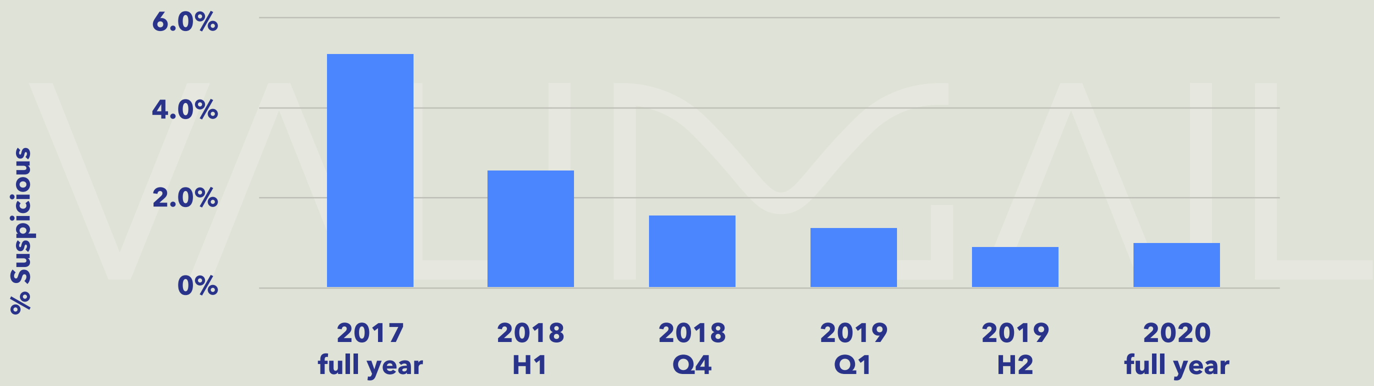
Global media companies and U.S. health care companies have the lowest rates of DMARC deployment and protection

SPOOFING RATES AND SOURCES

To get a read on the rate of domain spoofing among email traffic as a whole, Valimail examined consolidated data from millions of DMARC aggregate reports we collected on behalf of customers during 2020. Taken together, these represent hundreds of billions of individual email messages originating from tens of thousands of domains, sent to recipients using a wide variety of mailbox providers worldwide.

We found that, over the course of 2020, about 1 percent of all messages originated from suspicious and likely fraudulent senders. This is about the same as the rate we found in the second half of 2019. Given Radicati's estimate of overall email traffic worldwide, that translates to an average of 3 billion email messages using spoofed sender identities sent every day.

RATE OF SUSPICIOUS EMAIL



SOURCE: VALIMAIL, Q1 2021

(**Note:** The rate of domain spoofing was unusually high in 2017, reflecting the impact of a large impersonation campaign directed at media organizations that Valimail observed in late 2017, which makes that year's figure a bit of an outlier.)

Overall, the rate of domain spoofing appears to have leveled off after a period of decline over several years.

Interestingly, moving to DMARC enforcement not only stops these spoofs from being delivered, it also cuts down on the overall rate of attempted spoofing. We found that 1.9% of email from domains without DMARC enforcement is suspicious, while just 0.4% of email from domains with DMARC enforcement is suspicious.

In other words, domains without DMARC enforcement are 4.75x more likely to be the target of spoofing attempts than domains with DMARC enforcement.

Given that domains with DMARC enforcement are over-represented in the Valimail dataset, this means our estimate that 1% of the world's email traffic is using spoofing is almost certainly a conservative figure.

RECEIVERS ENFORCING DMARC

Given its benefits, it's no surprise that the growth of the DMARC standard has been impressive.

On the receiving side, major email receivers have been supporting the standard for several years. Valimail's data shows 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. This includes such well-known mailbox providers as Google (for both Gmail and Google Workspace, formerly known as G Suite), Microsoft (for both Outlook.com and Microsoft 365 accounts), Verizon Media (including Yahoo Mail and AOL), and many others. In addition, all the major enterprise gateways and secure email gateways (SEGs) do DMARC checks on inbound mail, usually by default.

Our data from analysis of DMARC reports shows that this 80% figure has remained fairly consistent over the past two years. There have been no major additions to the list of mail receivers doing DMARC checks on inbound mail. The most significant remaining outliers include a few large email providers in China as well as a number of smaller regional providers in Europe.

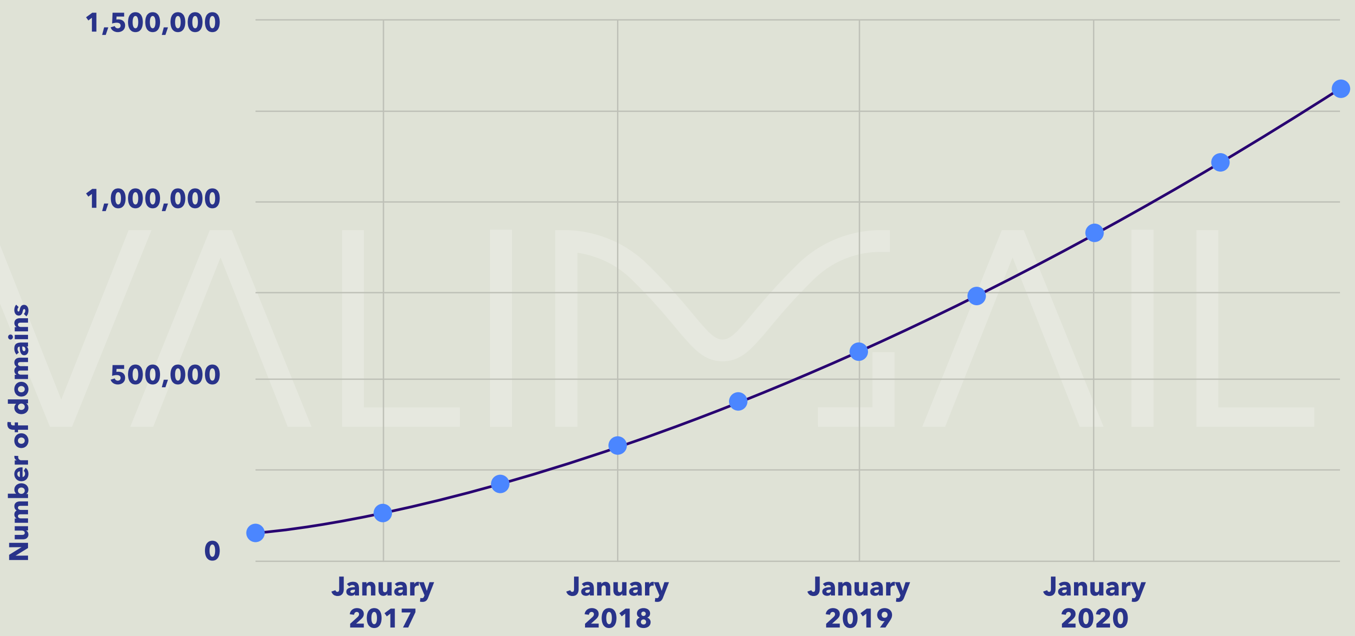
In short, DMARC checking — if enabled by domain owners — will be performed on inbound mail for the overwhelming majority of the world's estimated 7 billion active email inboxes.

TOTAL # OF DOMAINS WITH DMARC

On the sending side, more and more domain owners are waking up to DMARC's potential. At the start of 2021, Valimail found 1.28 million domains that have published DMARC records. (Note: This total excludes subdomains and is limited, to the best of our ability, to domains correlated with legitimate organizations of some kind.)

That's a 38% increase over the course of 2020, and it is 3.7x the number of domains with DMARC three years ago, at the start of 2018. The total crossed the psychologically significant threshold of 1 million domains in mid-2020.

TOTAL DOMAINS WITH DMARC



SOURCE: VALIMAIL, Q1 2021

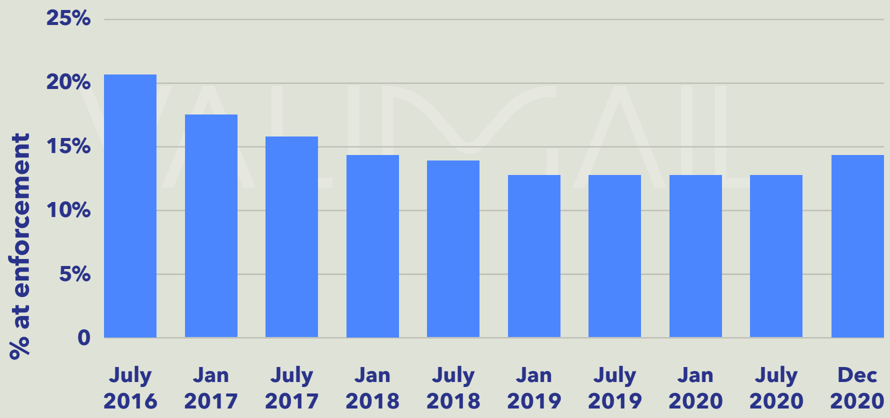
OVERALL ENFORCEMENT

Merely publishing a DMARC record is not sufficient to protect a domain against spoofing. Domain owners must also configure an enforcement policy. If they don't, then mail receivers will not take any particular actions on email that appears to come from the domain but which fails authentication — including malicious spoofs and phishing attacks.

Unfortunately, merely publishing a DMARC record in monitoring is as far as most domain owners get. Valimail's analysis shows that of the 1.28 million organizational domains with DMARC, just 14.8% are using an enforcement policy. In many cases, they have had DMARC records in place for years without ever changing to a more effective enforcement policy.

While low, this total is an increase over the past two years, when it stood at roughly 13.5%. Is this a sign that domain owners are starting to take enforcement more seriously? Time will tell.

PERCENT OF DMARC RECORDS AT ENFORCEMENT



SOURCE: VALIMAIL, Q1 2021

Among the 7,000 domains associated with large for-profit and government organizations that Valimail analyzed in detail for this report, Valimail found that 43.4% of all domains with DMARC were at enforcement — almost 3 times the internet-wide average. What's more, this is two percentage points higher than it stood in early 2020, and 3.5 percentage points higher than in early 2019. This indicates that DMARC enforcement is being taken more seriously among large organizations, and that they are proceeding, slowly but surely, to lock down even more of their domains with DMARC enforcement.

THE SYNTAX OF DMARC ENFORCEMENT

The DMARC standard lets domain owners specify a policy directive, instructing mail receivers how they should handle non-authenticating messages that appear to come from their domain.

"DMARC enforcement" is defined as a policy that directs mail receivers to quarantine or reject non-authenticated email, with no exceptions for subdomains.

However, domain owners who do implement such a policy without first carefully auditing their email environments run into trouble. If you don't properly authorize all the services that you want to send email on your behalf (e.g. a corporate payroll system, or mailing list manager) then the enforcement setting will tell mail servers to reject messages from those senders.

As a result, the best practice is to start in monitor mode (a policy of "none," also known as "monitoring mode"), which allows you to collect detailed, daily reports from mail servers about exactly which senders are authenticating and which ones are not.

Once you have collected sufficient data, you can then configure SPF and/or DKIM to specify which senders are allowed to send "as" you. Then, when ready, you can move to an enforcement policy.

For more on this topic, see "What is DMARC?" on the Valimail website.

INDUSTRY-SPECIFIC ANALYSIS

Diving deeper into the 7,000 domains for large organizations, we analyzed the aggregate DMARC status for each of 8 different industry categories.

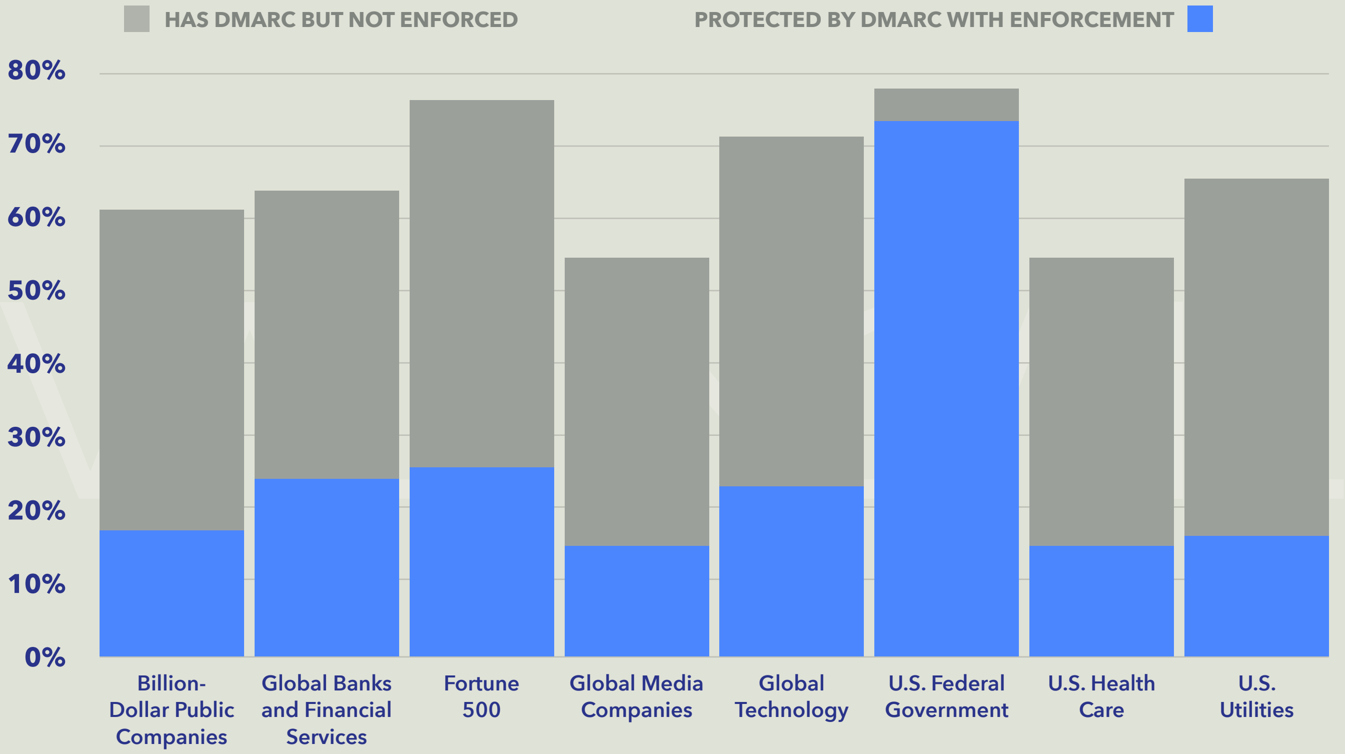
The U.S. federal government is still the undisputed leader in DMARC usage, with 78% of all federal domains having published a DMARC record, and 74% of those records having an enforcement policy. This means that 74% of federal domains are now protected from spoofing. This high rate of deployment and enforcement is a direct result of a 2017 directive from the Department of Homeland Security, BOD 18-01, which mandated DMARC enforcement for all executive branch domains, except for intelligence and defense related ones. The directive, while controversial, was met with a surprisingly high level of compliance, thanks in large part to the detailed documentation and enabling tools that DHS provided along with the order.

No other industry category comes close to the U.S. government in DMARC usage and effectiveness, as no other industry has seen the same kind of leadership (or regulation).

After the government, the category with the highest deployment of DMARC is the Fortune 500, of which 77% now have deployed DMARC. With only 27% of those domains having enforcement policies and actually protected from spoofing. In third place we find global technology companies, of whose domains 74% have DMARC records, and of whose DMARC records 24% have enforcement policies.

The category with the lowest rate of DMARC deployment is global media companies, of which just 57% have DMARC records; 16% of all global media companies are protected by DMARC at enforcement. However, it's actually U.S. health care companies that have the lowest rate of DMARC protection, thanks to a lower rate of enforcement: Just 13% of these companies have DMARC enforcement.

DMARC STATUS BY CATEGORY



SOURCE: VALIMAIL, Q1 2021

CONCLUSION

DMARC usage is growing, and rates of enforcement are increasing, as domain owners recognize the utility of this widely accepted standard for curtailing one of the most pernicious types of email-based attacks.

Deploying DMARC is typically a two-step process, in which domain owners first publish a DMARC record in monitoring mode, then later move to enforcement. While monitoring mode provides visibility into which services (and attackers) may be using your domain to send email, it is only with enforcement that you are able to shut down unauthorized senders and prevent them from reaching recipients' inboxes.

Overall, the vast majority of domains with DMARC are not yet at enforcement, but this rate is much higher among larger organizations, and is growing. As awareness grows about DMARC's effectiveness in locking down domains, we expect that these numbers will continue to increase.

TRUST YOUR EMAIL