AGARI

Agari Industry DMARC Adoption Report for Healthcare

Email Security in Critical Condition

Executive Summary

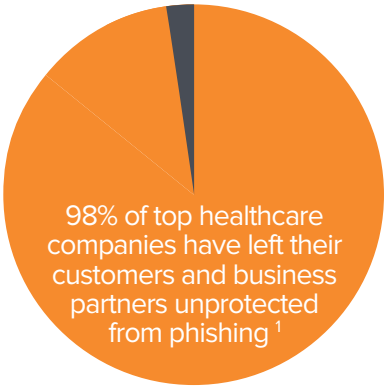
While email is one of the primary digital channels for client/patient interaction and digital engagement with customers, it has never been secure. Phishing attacks in the healthcare industry are more common than ever, with attackers regularly spoofing healthcare brands and leveraging them to hijack sensitive information directly from customers and patients.

DMARC is an email standard created some years ago to solve the spoofing and consumer phishing problem. A DMARC record, published alongside a domain's DNS records, ensures that only authorized senders can send email on behalf of an organization or domain.

In November 2017, Agari analyzed the DMARC authentication posture of 549 large organizations in the healthcare and pharmaceuticals sectors. We also compared the findings to an analysis performed six months ago with the same dataset. Key results and industry observations over this period include:

- **Attackers targeting healthcare more than other sectors:** Healthcare is the top-targeted sector, with over 92% of domains carrying fraudulent email over the period measured.
- **Healthcare sector overall remains a laggard in DMARC adoption:** As with the previous analysis, the overwhelming majority of healthcare organizations (77%) do not use DMARC. Of those that do, only 2% of organizations have enforcement-based policies in place to keep their customers from receiving inauthentic and/or fraudulent emails. A separate point-in-time analysis for member organizations of the NH-ISAC (National Health Information Sharing & Analysis Center) yielded marginally better results.
- **Positive change in enforcement policies:** While the overall percentage was low, there was an 85%increase in the total number of domains at enforcement over the period we measured.
- **Industry developments likely to drive more adoption:** On October 16th, the US Department of Homeland Security (DHS) issued a landmark binding directive ordering federal agencies to adopt DMARC, mandating a specific date for full enforcement. The NH-ISAC responded almost immediately asking members to take a pledge to adopt DMARC in 2018.

This report summarizes the DMARC adoption details for the healthcare industry and cites results from forward-thinking organizations who have implemented DMARC to protect their customers and brand.



[1] Source: Public DNS record analysis on primary corporate website domains for global healthcare / pharmaceutical companies with revenues above $1B. Analysis conducted on November 7th 2017.

Email Abuse on Healthcare Domains

Heatlhcare is a target-rich environment for attackers, who value the sector because of the prevalence of patient records that contain personally identifiable information (PII) like Social Security numbers and credit card information for billing that could be used for future identity theft. Accordingly, this year's Verizon 2017 Data Breach Investigations Report listed the healthcare as the second-most affected from a security incident perspective, trailing only the finance sector.[2]

Together with these high-profile targeted attacks that have breached corporate networks, criminals are executing phishing attacks leveraging the brand name of healthcare organizations. For attackers, the same motivations and attractions exist when targeting a healthcare organization's customers as they do with an organization's employees. A phishing message that exploits a trusted healthcare organization's brand and spoofs their domain can just as easily lead to compromised patient data when the unsuspecting recipient opens the messages and falls for the con.

The following snapshot of threat activity over Agari healthcare customer domains highlights the issue in stark terms: more than half of emails patient receive are fraudulent. Note that this number has spiked almost 50% on certain weeks over the past six months.

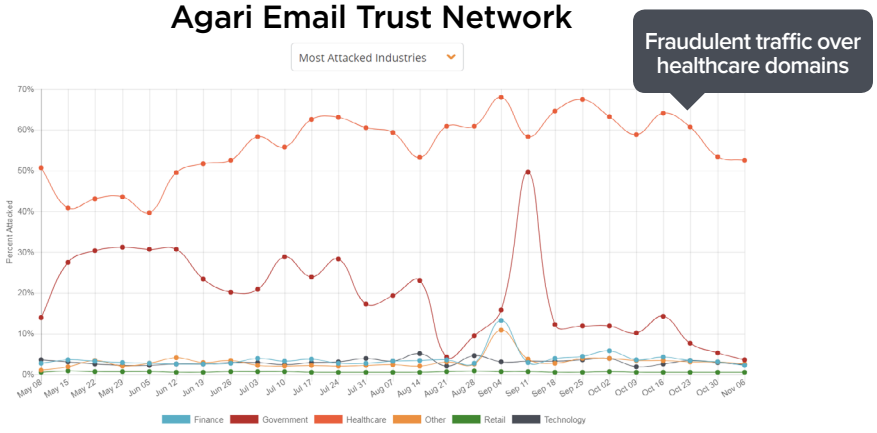
Agari Email Trust Network

Agari Protected	Threat Volume	Threat Rate
874.6 M Total Emails	498.21 M Malicious Emails	56.96% Malicious Emails
1,911 Total Domains	1,774 Domain Targeted	92.83% Domain Targeted

Over 50% of email "from" healthcare organizations is fraudulent

To analyze the latest email fraud stats for healthcare and other sectors, visit **agari.com/email-threat-center/**

In an interesting parallel, across Agari's entire customer base, which, over the past six months accounted for over a trillion messages sent, healthcare domains were the single most targeted for fraudulent email or phishing. The volume of fraudulent or otherwise unauthenticated email on healthcare domains was almost 3 times the next nearest sector, which was government.



#2

Rank of healthcare among sectors affected from security incidents.
Verizon Data Breach Report, 2017

#1

Rank of healthcare among sectors with domains targeted with unauthenticated mail.
Agari Email Threat Center 6 month period ending Nov 7, 2017

Most Attacked Industries

Healthcare	57
Government	19
Finance	4
Other	3

[1] 2017 Data Breach Investigations Report http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

DMARC Adoption in the Healthcare Industry

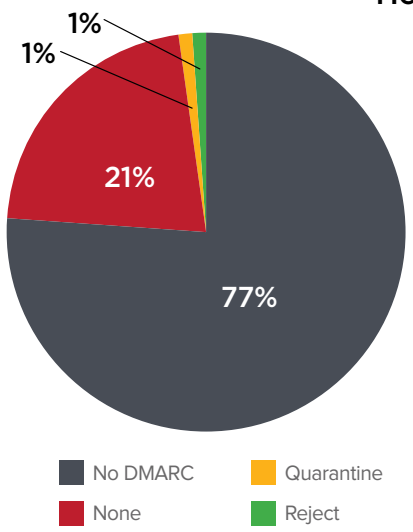
The definitive way to address abuse targeting an organization's email-sending domain is to implement authentication, specifically DMARC. When a company implements DMARC, there are three levels of policies that can be applied to their domains:

Monitor (None) – Unauthenticated messages are monitored but still delivered to the recipient's inbox
Quarantine – Unauthenticated messages are moved to the "Spam" or "Junk" folders
Reject – Unauthenticated messages are blocked and not delivered to any folder. This is the ideal state to achieve.

For more information on the DMARC standard, see www.agari.com/dmarc-guide/

On November 7th, 2017 Agari conducted an analysis of public DNS records for primary corporate website domains of global healthcare / pharmaceutical companies with revenues above $1B. Within this set of large healthcare organizations, Agari found that overwhelming majority had no DMARC record at all. Of those that did have a record in place, most had no policy implemented to take action against fraudulent emails. While they are a tiny minority, some healthcare organizations are aware of the threat of digital deception and have taken appropriate counter-measures, notably moving their DMARC configuration to a Reject policy. Achieving reject is important because only then are mailbox providers instructed to refuse any malicious emails purporting to be from their brand.

Healthcare Industry DMARC Adoption



DMARC adoption – More than 77% of healthcare organizations (421) do not have a DMARC record on their domains. It's notable that this low adoption rate trails what Agari has recently reported for the commercial sector, where two-thirds (67 percent) of Fortune 500 have not published any DMARC policy on their domains.

None Policy – 21% of healthcare organizations have a none (Monitor) policy. This policy monitors for authentication abuse, but does not prevent it. When combined with the number of domains without any DMARC policy, we can conclude that almost 98 percent of healthcare organizations are vulnerable to digital deception, leaving their constituents and email recipients exposed to phishing and fraud.

Quarantine Policy – Approximately 1 percent (6 organizations) implemented a Quarantine policy, which redirects messages failing authentication to the configured spam folder.

Reject Policy – Another 1% (8 organizations) have implemented a Reject policy to block messages that fail authentication.

While the number domains at enforcement level (Quarantine and Reject) is relatively low, the 6 month trend is encouraging, as shown in the following table.

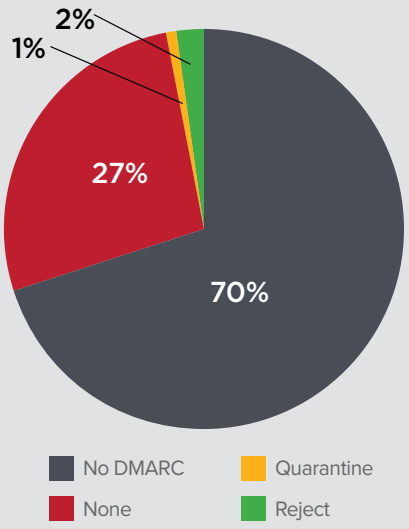
Enforcement Changes on Healthcare Domain Over 6 Months

	Domains at Quarantine	Domains at Reject
May 2017	2 Bruker Corporation Sharp HealthCare	5 Aetna Inc. Flex Geisinger Health System HealthNow New York, Inc. Houston Methodist
Nov. 2017	6 200% ▲ Bruker Corporation **Gilead Sciences, Inc.** **Kettering Health Network** Sharp Healthcare **Sun Pharmaceutical Industries Ltd** **Tampa General Hospital**	8 33% ▲ Aetna Inc. **Blue Shield of California** Flex Geisinger Health System HealthNow New York, Inc. **Horizon Blue Cross Blue Shield of New Jersey** Houston Methodist **Spectrum Health**

Industry snapshot: The NH-ISAC

The National Health Information Sharing & Analysis Center (NH-ISAC) is the official health care information sharing and analysis center. With a membership mix including healthcare providers, insurers, pharmaceuticals, biotech, and others, the overarching goal of the NH-ISAC is to promote cybersecurity in the Healthcare and Public Health (HPH) sector. Given the vital role the HPH serves in the nation's critical infrastructure, embracing DMARC controls within this ecosystem is logical step to eliminate domain spoofing as a phishing technique for patients and consumers.

NH-ISAC DMARC Adoption: Slightly outpacing the larger Industry



On a percentage basis, the membership of the NH-ISAC is ahead of the superset of large healthcare organizations when it comes to implementing DMARC.

In keeping with the larger trend, the majority (70%) of NH-ISAC members have no policy at all. However, this represents a 7% improvement over the industry at large that we analyzed. Focusing on rest of the NH-ISAC group that does have a DMARC policy, the distribution of policies is higher across with board, notably with the all-important Reject policy for enforcement (2% vs. 1% for the industry at large.)

These marginal improvements notwithstanding, the overall adoption numbers are low for this group, especially considering the security risk of fraudulent or otherwise unauthenticated email traversing healthcare domains.

The DMARC Pledge: First Steps to Broader Adoption

On October 16th, 2017, the Department of Homeland Security (DHS) directed all federal agencies to implement better security protocols on government emails and websites by implementing DMARC. That same week, Jim Routh, Chairman of the NH-ISAC, issued a letter enlisting NH-ISAC member to take a "pledge" to implement DMARC. Below is an excerpt from that request:

> *I am asking you to make a pledge to implement DMARC in 2018 on behalf of your organization in an effort to dramatically improve cyber resilience for healthcare. I implemented DMARC three years ago for my enterprise and we continue to get a 10% lift in click-through rate for all external emails each year as a key indicator of the increase in trust from our members.*

The pledge is an important first step for many NH-ISAC members, demonstrating the commitment to making measurable improvise in email security for the HPH community. For more information on the pledge, see https://www.surveymonkey.com/r/JCKLCYD

A Brief History of Email Authentication

DMARC emerged from an experiment piloted by Yahoo! and PayPal in 2007 that was designed to prevent account credential phishing. Before DMARC, there were two email authentication protocols, "Sender Policy Framework" (SPF) and "Domain Keys Identified Mail" (DKIM). SPF utilizes DNS to specify which mail servers are authorized to send email for the domain listed in the envelope or "bounce" address. SPF is therefore able to authenticate the envelope sender, but does nothing to authenticate the sender contained in the "From: header" of the message. Since end users don't see the envelope sender, it's far more important to authenticate the "From: header," which they do see.

DKIM uses cryptographic authentication. A hash of the message is digitally signed using a private key known only to the sending email server. This signature rides around in a special message header, and can be verified using the signer's public key, which is stored in the signer's DNS. DKIM is actually quite easy to deploy so long as your mail server or Email Service Provider supports it. Unfortunately,

there's a misconception that DKIM is difficult to deploy, or that deploying DKIM will cause receivers to block your email if the signature fails validation. Neither of these are true.

The "Domain-based Message Authentication, Reporting & Conformance" (DMARC) protocol seeks to advance these previous standards by comparing the envelope sender authenticated by the SPF check and the signing entity authenticated by the DKIM signature back to the sender listed in the "From:" header. Known as "identifier alignment", this identifier comparison is what enables DMARC to authenticate the "From: header" of an email message.

PayPal and Yahoo! were successful in their DMARC pilot program. Criminals could no longer send fraudulent PayPal messages to Yahoo! mail users. Next came a working group of email industry experts including Google, Yahoo!, Bank of America, PayPal, Agari, and a number of other companies interested in scaling up the Yahoo!/PayPal experiment. The goal was to allow anybody on the Internet to control the use of their domain in the "From:" header of email messages. This group was known as MOOCOW, or Messaging Operational Overlay Coalition Of the Willing.

After many months of discussion, debate, and compromise, Microsoft, AOL, Google, and Yahoo! deployed the first working receiver implementations of what came to be known as DMARC in January 2012. Since then, many senders and receivers have implemented this crucial email control, often with the help of a vendor such as Agari. In March 2015, DMARC was detailed in an informational Request for Comments as RFC-7489. Since then, a number of additional consumer mailbox providers have implemented the standard, and most major Secure Email Gateway vendors have incorporated parts of the standard into their services and appliances.

DMARC is designed to be deployed in stages. Companies generally start in "monitor mode" using what's known as a "p=none" policy. This will provide feedback about servers using the domain name in the "From:" header of the email messages they send. The domain owner uses this information to make adjustments to their SPF and DKIM configurations until all of their legitimate mail sources are properly authenticated. At this point, the policy can be tightened to "p=quarantine", which sends authenticated messages to the recipient's spam folder or even "preject", which causes the message to be blocked outright.

According to DMARC.org, DMARC is designed to:

- Minimize false positives.
- Provide robust authentication reporting.
- Assert sender policy at receivers.
- Reduce successful phishing delivery.
- Work at Internet scale.
- Minimize complexity.

Finally, it is important to realize that DMARC must also be deployed on the receiver side, by email service providers. Currently, the major email service providers, Microsoft, AOL, Google and Yahoo! have deployed DMARC, but smaller email service providers or a self-hosted email server may not provide the same level of protection.

A Practical Deployment of DMARC

Agari is uniquely positioned to share its insight into the practical applications of DMARC deployments because so many of its users are early adopters of DMARC. The following charts provide an anonymized view of Agari dashboards to highlight the positive impact of DMARC. Together, Agari and DMARC are preventing digital deception

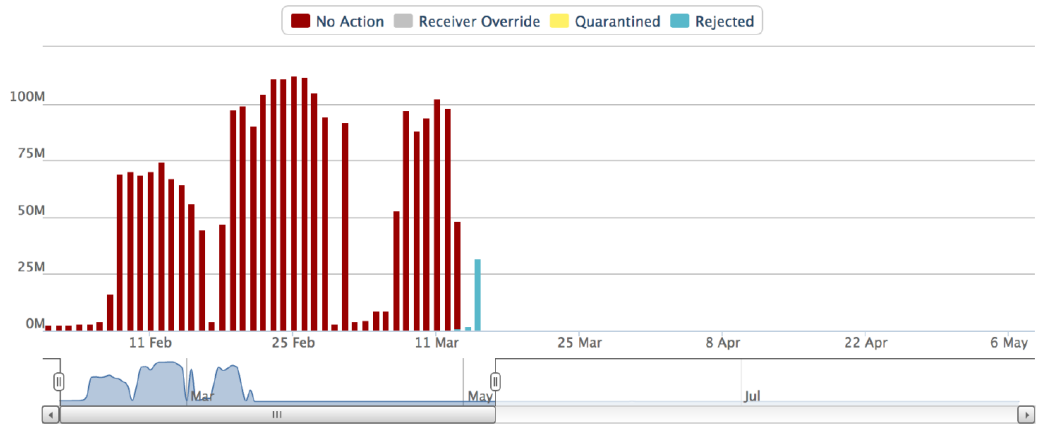


Figure 5 – DMARC Pre and Post Reject

As shown in Figure 5, the Agari client was receiving a tremendous volume of unauthenticated emails – at times more than 100 million per day. These are emails that were spoofing the domain in the "From:" header. Shortly after March 11, 2013, the client implemented a DMARC Reject policy, resulting in millions of spoofed messages that could no longer be delivered. As a result, by the end of that March, these messages all but ceased – the perpetrators realized there was no benefit to continue their campaign when every message was rejected.

Following this same customer's journey, let's fast forward a few years.

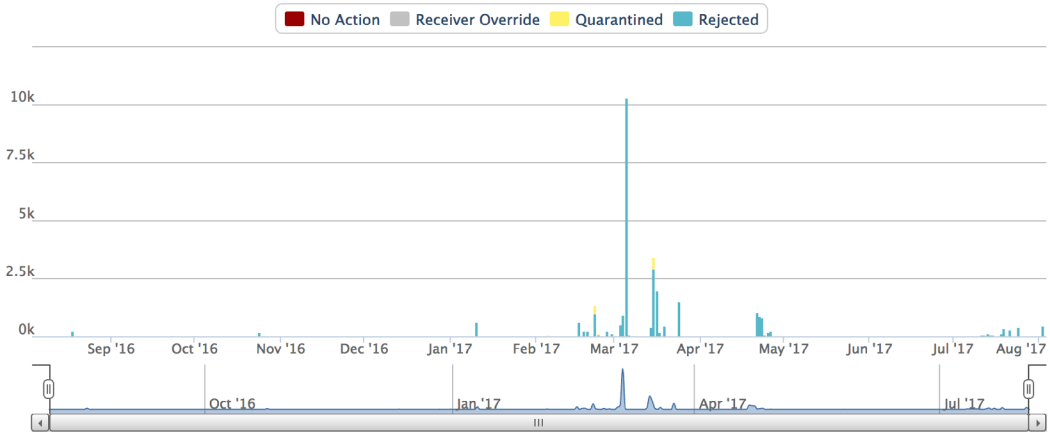


Figure 6 – DMARC Reject

Figure 6 demonstrates that these spoofed messages have been all but eliminated. In most cases, there are simply no messages that are attempted to be sent. However, every so often, a new campaign may emerge, as seen in March of 2017. Even in this instance, the volume of messages sent is only 10,000, which seems insignificant compared to the initial 100 million. Again, these messages are rejected and the campaign drops off, as attackers turn their attention to more vulnerable targets elsewhere. DMARC is so effective at preventing these campaigns that the bad guys literally give up trying.

Finally, let's switch gears to observe the gradual deployment of DMARC from Monitor (None) to Quarantine, to Reject.

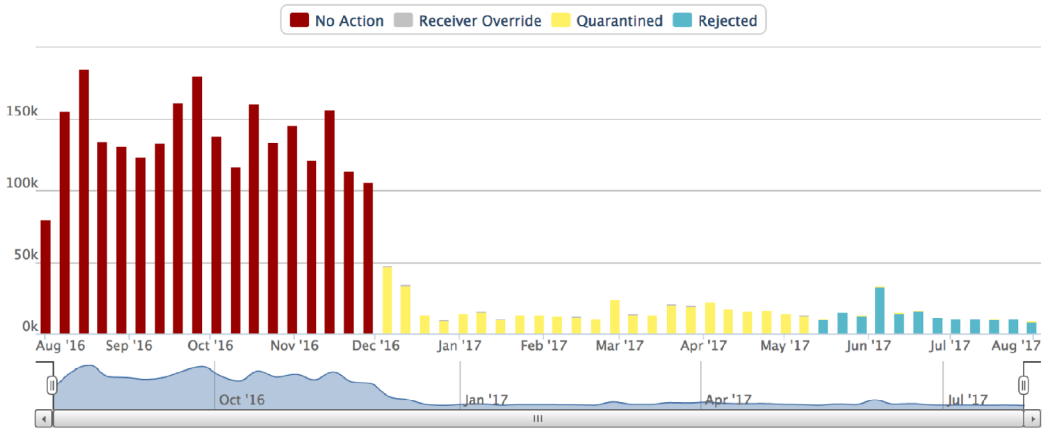


Figure 7 – DMARC Monitor (None), Quarantine and Reject

Figure 7 demonstrates another client's gradual adoption of tighter DMARC policies, precisely as DMARC was designed to be deployed. The initial volume of unauthenticated mail surpassed 100,000 to 150,000 messages per day, which was cut dramatically to 50,000 or less once a Quarantine policy was implemented. After another six months, this is tightened further to a Reject policy, which practically eliminates the volume of unauthenticated email.

Based on the Agari research, many organizations find themselves in the first stage of DMARC implementation and unable to progress to quarantine and reject policies. The reason for this is that larger organization have to first identify who is sending email on their behalf and get them to authenticate the email they are sending before changing the policy. Agari is the leading solution to help large organization with the analytics, workflow and services to move to more effective policies, maintain email governance and prevent ongoing brand abuse.

Conclusion

The analysis in this report has shown that healthcare organizations are woefully unprotected against phishing. Almost 98% of organizations in this sector either do not have a DMARC policy or maintain a monitor-only policy that doesn't protect their customers. With only 2% of organizations enforcing protection against unauthenticated traffic using their domain names or from those who send on their behalf, virtually the entire healthcare customer base remains vulnerable to domain spoofing and phishing attacks. Agari Threat Center data also showed that more than half of emails patient receive are fraudulent. This rate has been steadily increasing over the past six months.

Fortunately, momentum appears to be shifting in the right direction. On the heels of a directive issued by the US Department of Homeland Security mandating the adoption of DMARC on a wide swath of the US government email-sending domains, the NH-ISAC recently called on its members to take a "DMARC Pledge". This pledge encourages member organizations to commit to the configuration of DMARC controls following the same time to which their counterparts in the federal government are subject. Such efforts are encouraging, as increasing DMARC adoption in the healthcare sector is key to defeating malicious actors that abuse the trust and brand reputation these same organizations have spent years building.

Take the NH-ISAC DMARC Pledge: **nhisac.org/DMARC-pledge**
Create or look up a DMARC record **agari.com/resources/tools/dmarc/**
Contact Agari to help protect your customers with DMARC: **agari.com/contact-us**

About Agari
Agari, a leading cybersecurity company, is trusted by leading Fortune 1000 companies to protect their enterprise, partners and customers from advanced email phishing attacks. The Agari Email Trust Platform is the industry's only solution that 'understands' the true sender of emails, leveraging the company's proprietary, global email telemetry network and patent-pending, predictive Agari Trust Analytics to identify and stop phishing attacks. The platform powers Agari Enterprise Protect, which help organizations protect themselves from advanced spear phishing attacks, and Agari Customer Protect, which protects consumers from email attacks that spoof enterprise brands. Agari, a recipient of the JPMorgan Chase Hall of Innovation Award and recognized as a Gartner Cool Vendor in Security, is backed by Alloy Ventures, Battery Ventures, First Round Capital, Greylock Partners, Norwest Venture Partners and Scale Venture Partners. Learn more at http://www.agari.com and follow us on Twitter @AgariInc.