FORTRA

REPORT

2022 Email Fraud & Identity Deception Trends

The State of DMARC Enforcement

Inside This Report

The intelligence presented in this report reflects data captured via the following sources in 2021:

Active defense engagements with **cyber threat actors** to gather intel about emerging BEC tactics and targets

Data extracted from **trillions of emails** analyzed and applied by Agari Identity Graph

DMARC-carrying domains identified among **426 million** domains crawled worldwide

Incident data from SOC professionals in a **survey of large enterprises** averaging 21,000 employees and spanning multiple industries

Agari Cyber Intelligence Division (ACID) was the first-of-its-kind world's only counterintelligence research group dedicated to business email compromise (BEC) investigation and cybercrime abatement. Since May 2019, ACID conducted more than 12,000 active defense engagements with threat actors, working closely with CISOs at global enterprises, law enforcement, and other trusted partners to stop identity-based phishing and socially-engineered cybercrimes.

Table of Contents

Executive Summary

Two years into the pandemic and amidst too many successful cyberattacks to keep count, cyberccrime remains to be a constant battle. In 2021 alone, email spoofing and phishing increased by 220%.[1] And despite billions having been invested into perimeter and endpoint security over the last two years, phishing and business email compromise (BEC) scams continue to be the primary attack vectors into organizations, often giving threat actors the toehold they need to wreak havoc on companies and their customers. In fact, over $44 million in losses in 2021 were a direct result of successful phishing and advanced email scams.[2] As corroborated in this latest analysis from the Agari Cyber Intelligence Division (ACID), the success of these attacks is much more reliant on savvy social engineering ploys that easily evade most of the email defenses in use today.

Global adoption of Domain-based Message Authentication, Reporting, and Conformance (DMARC) leapt 19% from 2020-2021. However, the number of Fortune 500 companies to deploy DMARC policies showed a mere 10% increase with DMARC set at its most aggressive level of enforcement, namely at p=reject. While any rise in that number is encouraging, it means 66% of the nation's most prominent companies remain at risk of impersonation in phishing attacks targeting their customers and the general public. But far more promising news showed a 96% rise in the number of brands adopting Brand Indicators for Message Identification (BIMI) at a time when the email channel is more crucial and relied upon by companies for communication than ever before.

KEY FINDINGS

37%
The percentage of global domains at the highest level of DMARC enforcement in 2021, a number that reached almost 4.8 million—up from 3.8 million in 2020

2 in 3
Today, 66% of Fortune 500 companies remain vulnerable to getting impersonated in phishing scams targeting their customers, partners, investors, and the general public

96%
The increase in brand domains that have BIMI records, which reached 18,913 in the fourth quarter of 2021—up from 11,827 in Q1 2021

DMARC Adoption Snapshot

The Industry's Largest Ongoing Study of Adoption Trends Worldwide

In a snapshot of hundreds of millions of Internet domains, we analyzed adoption trends for Domain-based Message Authentication, Reporting, and Conformance (DMARC) from January through December 2021.

Nearly 13 Million

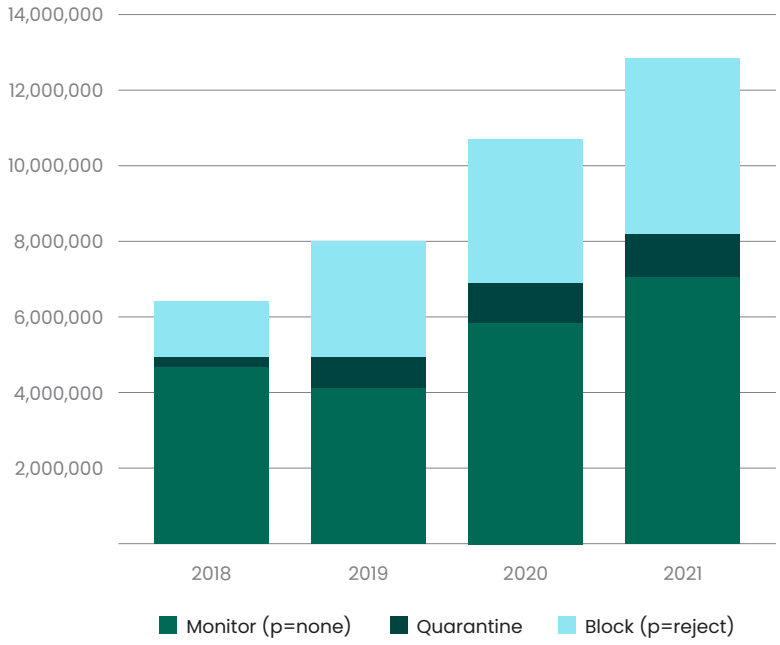
The Number of Domains With Recognizable DMARC Policies Worldwide—up 19% from 2020

But don't break out the champagne just yet. While this notable increase in the number of domains with an identifiable DMARC policy is encouraging, it still represents just a tiny fraction of the half-billion domains our researchers scanned worldwide.

Nearly 4.8 Million

Domains Have DMARC Set to Its Highest Enforcement Level—a 24% Increase from 2020, But Still Low in Absolute Numbers

Failure to implement DMARC with the p=reject enforcement leaves organizations at risk from cybercriminals seeking to pirate their brand and domains to target phishing attacks at their customers and other consumers and businesses. These domains may also be blacklisted by receiver systems or may experience reduced deliverability rates for the brand's legitimate email messages, resulting in costly disruptions to their email-based marketing and revenue streams.



Growth in Number of Domains with DMARC Policies, 2018–2021

DMARC Breakout: Region

As part of this report, ACID examines the state of DMARC adoption by key geographies in 2021.

Top 2

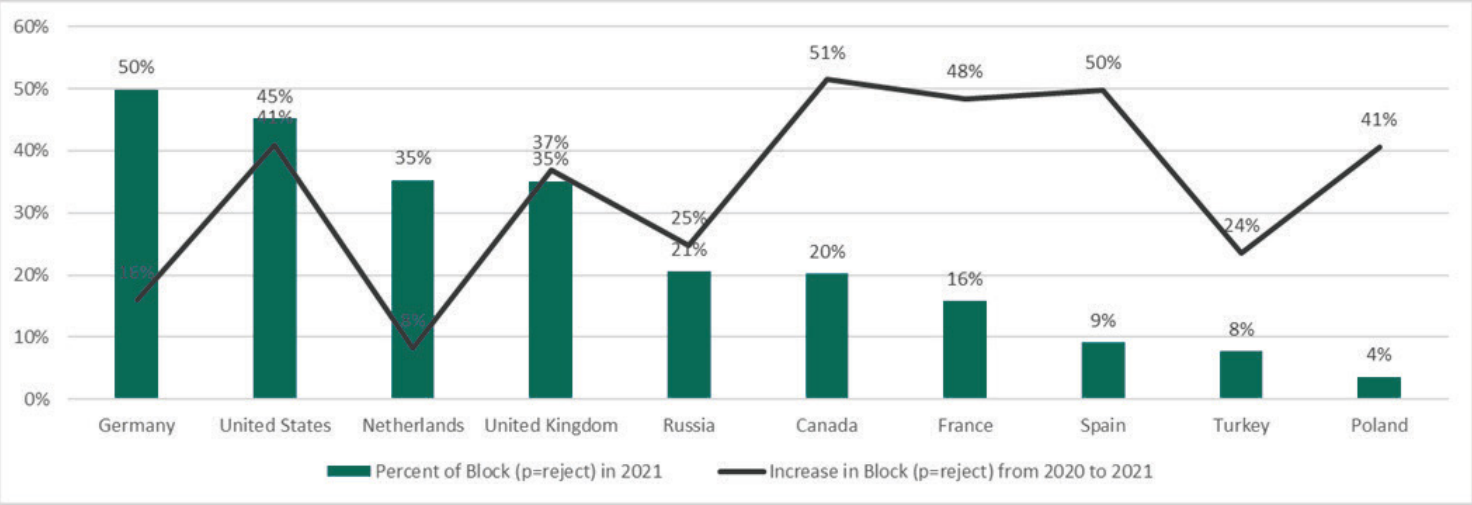
Similar to 2020, Germany and the US Still Lead the Pack with DMARC Policies Set at Full Enforcement

Among the ten largest country-code domains, the United States racked up a 41% increase in the percentage of domains with DMARC policies set to the strictest possible enforcement level in the last year, as compared to Germany which only achieved a 16% growth in DMARC policies at full enforcement from 2020. However, Canada showed up strongly as it more than doubled the strictest possible enforcement level in 2021.

40%

Countries with This Rate of Growth or Higher in Setting the Strongest Enforcement Level

After Canada and the United States, the countries rounding out the top 5 highest amount of growth in DMARC Reject policies were Spain, France, and Poland.



Increase in At-Reject Levels for 10 Largest Country-Code Domains from 2020-2021

DMARC Breakout: World's Largest Companies

This report captures DMARC adoption trends among some of the world's most prominent companies throughout 2021—including HDAX, the Fortune 500, the FTSE 100, and the ASX 100. It's important to note that even when organizations have assigned DMARC records to their domains, they are not truly protected unless they are set to a level of enforcement. The sizable proportion of "no record" and "monitor only" policies highlights the fact that these organizations can still be impersonated in phishing campaigns that put their customers and other consumers and businesses at risk of serious financial harm.

34%

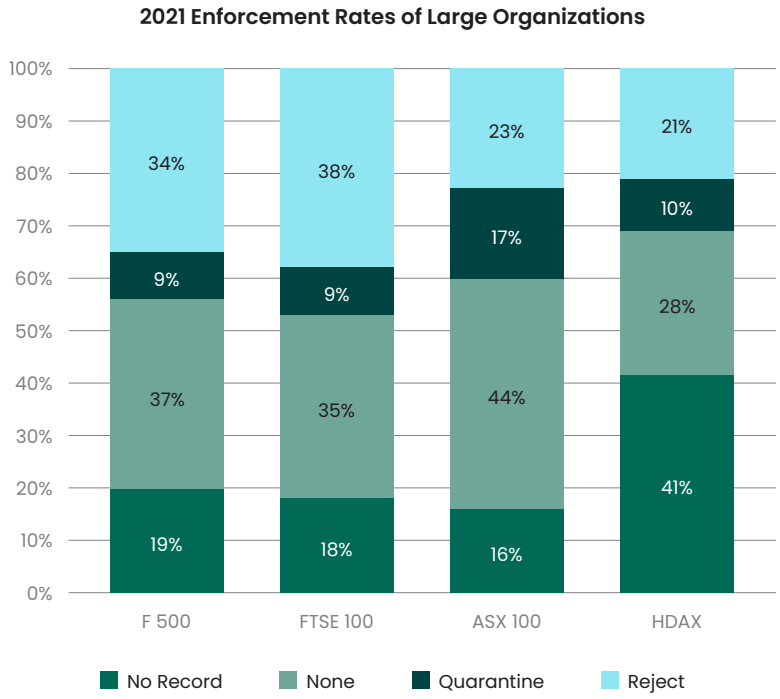
Fortune 500 Companies with DMARC Set at Full Enforcement to Prevent Domain Spoofing

That's an increase of 10% from 2020. Together with the 9% of DMARC-assigned domains with a p=quarantine policy, 43% of Fortune 500 domains with DMARC policies set with at least some level of protection rose 11% during the same period in 2020.

2/3

Fortune 500 Companies Remaining at Risk of Being Impersonated in Email Scams Targeting Customers, Partners & More

With the last 2 years of COVID-19 and its global effects, and the tribulations that trickled down for corporations, it's alarming to think that 66% of Fortune 500 companies STILL lack the protection needed to prevent email threat actors from hijacking their domains and impersonating their brands in phishing attacks. Which may help explain why Gartner ranked DMARC implementation[3] as a top priority for every organization in 2021.



DMARC Breakout: World's Largest Companies

MORE THAN 1/3

FTSE 100 Companies Protected Against Brand Impersonation—a 13% Increase

The number of companies on the UK's FTSE 100 with domains protected by DMARC set to p=reject grew to 38% in 2021—up from 25% in 2020. While commendable, it still means that 62% of the FTSE 100 does not yet have protections in place to prevent threat actors from impersonating their brands in email attacks targeting customers, investors, and the general public.

77%

Number of Australia's ASX 100 Companies That Continue to Put Customers at Risk

Amid a push to increase the number of Australian government domains protected by DMARC[4], the private sector is still struggling with deployment, even as the total number of domains in use continues to rise. Today, 23% of ASX 100 companies have DMARC policies set to full enforcement—leaving more than three-quarters at risk of email threat actors pirating their domains for use in phishing attacks.

21%

HDAX Companies with DMARC Policies Set to Full Enforcement

A sustained onslaught of malware and ransomware attacks in 2021 led to Germany's Federal Office for Information Security (BSI) issuing a nationwide red-alarm level warning for cybersecurity threats.[5] Thus, it is not surprising that the number of domains in the country at reject level went up from 9% in 2020 to 21% in 2021. Despite this upward trend, as well as another 10% at quarantine level, a whopping 69% of HDAX companies were left vulnerable to abuse by fraudsters.

DMARC Breakout: Industry Vertical

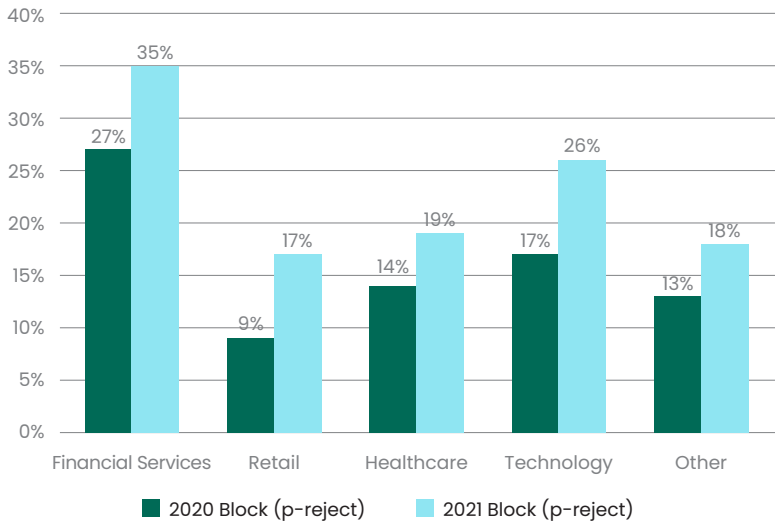
Financial & Technology/SaaS Providers Most Impersonated in Phishing Attacks

Putting an exclamation point on the need for DMARC protection: During the 4th quarter of 2021, the financial sector, webmail and software-as-a-service (SaaS) providers, and cryptocurrency exchanges and wallet providers were impersonated most in phishing attacks leveraging unprotected email domains.[6] None of which is surprising, given the ongoing COVID-19 pandemic and the resulting 70% of full-time corporate employees working from home.[7] This, on top of politically charged worldwide events, led to a spike in every category of cyberattack over the course of 2021. However, a positive that came out of this was every key industry's push to strengthen their DMARC enforcement level in 2021.

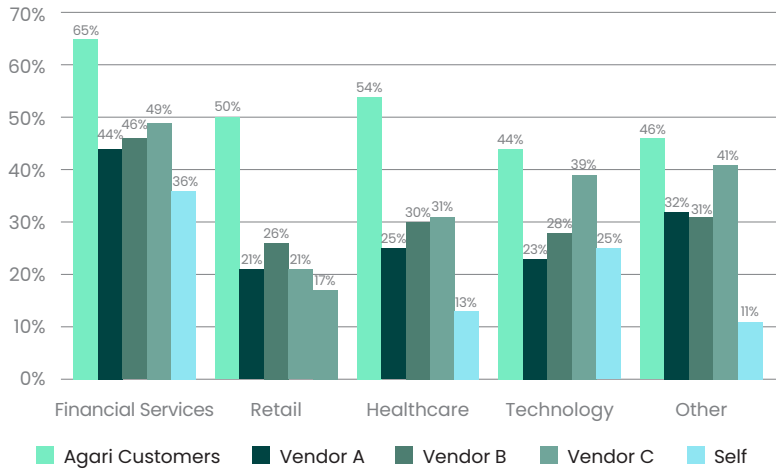
Agari Still Leads Pack for the Most Customer Domains at Reject Level in the Financial Services Sector

In one of the most competitive verticals which also has the best handle on implementing DMARC enforcement—Financial Services—Agari customers dominated our competitors' customers in getting their DMARC enforcement level to reject. In fact, 65% of Agari customers attained the strongest level of enforcement in 2021 as compared to our top 3 competitors in the landscape, who averaged 46.3% versus those who tried to implement it themselves, who also lagged at 36%.

Percent Total Domains at Reject by Industry



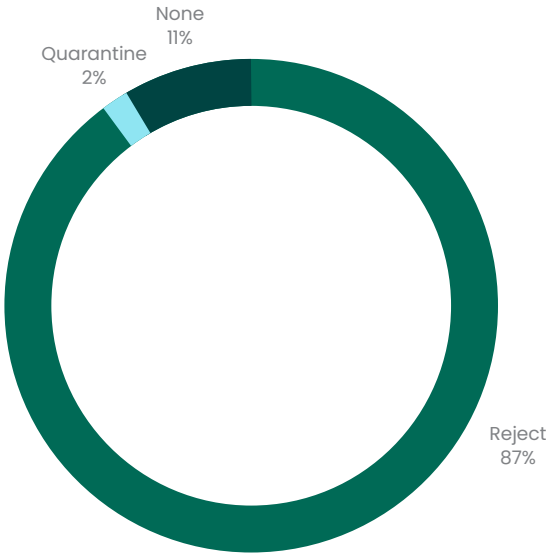
Vendor Comparison of Domains at Reject by Industry



DMARC Breakout: Industry Vertical

The Agari Advantage: Industry Enforcement Comparison

The Agari Email Threat Center's detailed set of DMARC data enabled ACID to measure how enforcement rates across industries compared with those of Agari customers and found that they were at an all-time high of 87% at p=reject level, up 6% from 2020's study. However, a positive that came out of this was every key industry's push to strengthen their DMARC enforcement level in 2021.



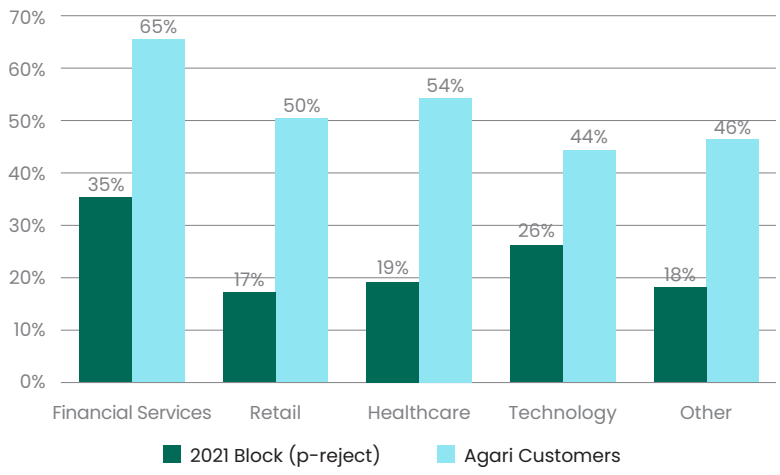
DMARC Enforcement Rate for All Agari Customers, 2021

NEARLY 3X Agari Healthcare Industry Customers with Domains at Full DMARC Enforcement vs. the Industry Average

The healthcare industry continued to be a leading target for data breaches and phishing attempts. After 2020, in which nearly 12 billion pieces of protected health information was exposed, the Health and Human Services (HHS) Leak Portal recorded 325 new data leaks affecting at least 500 pieces of protected health information in the first half of 2021 alone.[8]

From phishing campaigns impersonating American Anesthesiology, Inc. to nationwide healthcare authorities, Agari customers in the sector had ample reason to beef up DMARC implementation efforts. As of December 2021, 54% of Agari healthcare customers' domains are set at a p=reject enforcement level. That's nearly 3X the industry average of only 19% of domains protected with DMARC at its highest enforcement level.

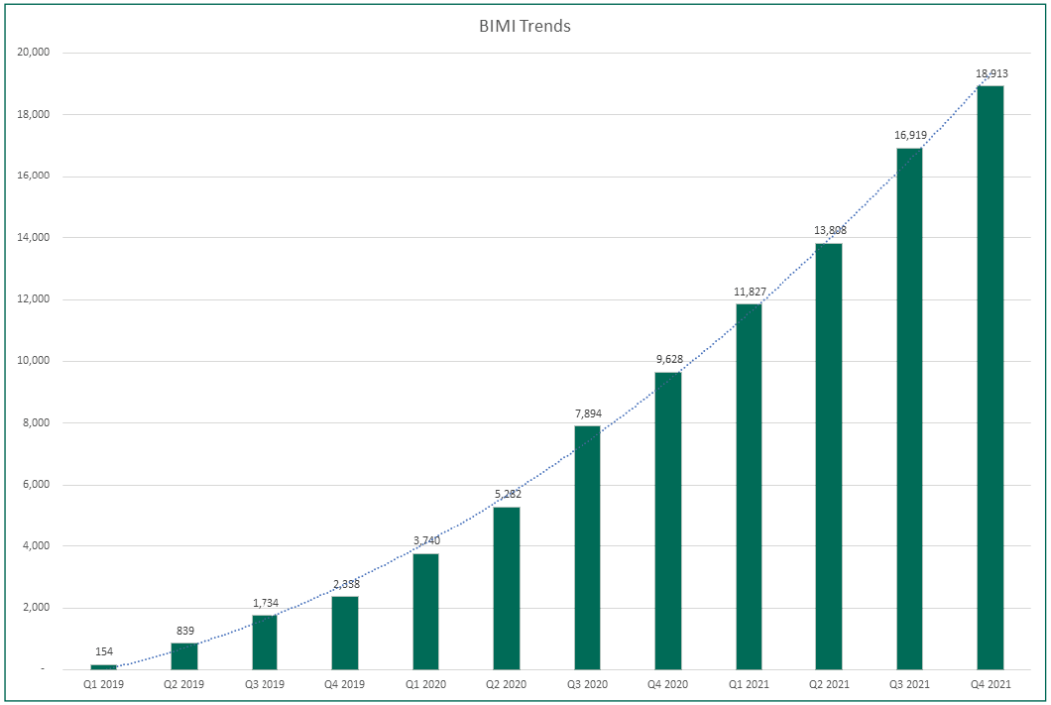
Share of Industry Domains at Strong DMARC Enforcement



Brand Indicators Adoption

BIMI Adoption Continues to Boom

Brand Indicators for Message Identification (BIMI) benefits the entire email ecosystem by providing businesses with a standardized method for publishing their verified brand logos next to their email messages within a recipient's inbox, validating that it comes from an authentic domain. This safeguards the recipients and protects them from brand spoofing or phishing attacks.



Quarterly Growth in Number of Domains with BIMI Record, 2019–2021

18,913

The Total Number of Brand Domains with BIMI Records as of December 31, 2021

BIMI only works with email that has been authenticated through the DMARC standard for which the domain owner has specified a DMARC policy enforcement, so only authenticated email messages can be delivered. DMARC has been shown to boost deliverability rates. This report shows that BIMI continues to gain additional mindshare and trust from users.

96%

Increase in Brand BIMI Adoption Over the Last 12 Months

From the end of 2020 through the end of 2021, BIMI adoption grew 96% from just 9,628 in 2020. In fact, since the successful rollout of Google's high-profile BIMI pilot in mid-2020, BIMI is now supported by Yahoo, Verizon Media, and Fastmail (among others) and is accessible to billions of inboxes, cementing email's role as the indispensable digital channel to marketers with built-in protections against brand spoofing and phishing attacks.

Protecting Against Advanced Email Threats with Agari DMARC Protection

As the financial and reputational damage from phishing, BEC, and other advanced email threats continue to mount, Agari has become a market leader in protecting brands and people from devastating, costly, and socially engineered phishing attacks. We accomplish this by:

- Automating DMARC email authentication and enforcement
- Simplifying the process and providing continuous monitoring and threat mitigation
- Preserving brand identity and boosting digital engagement with your brand

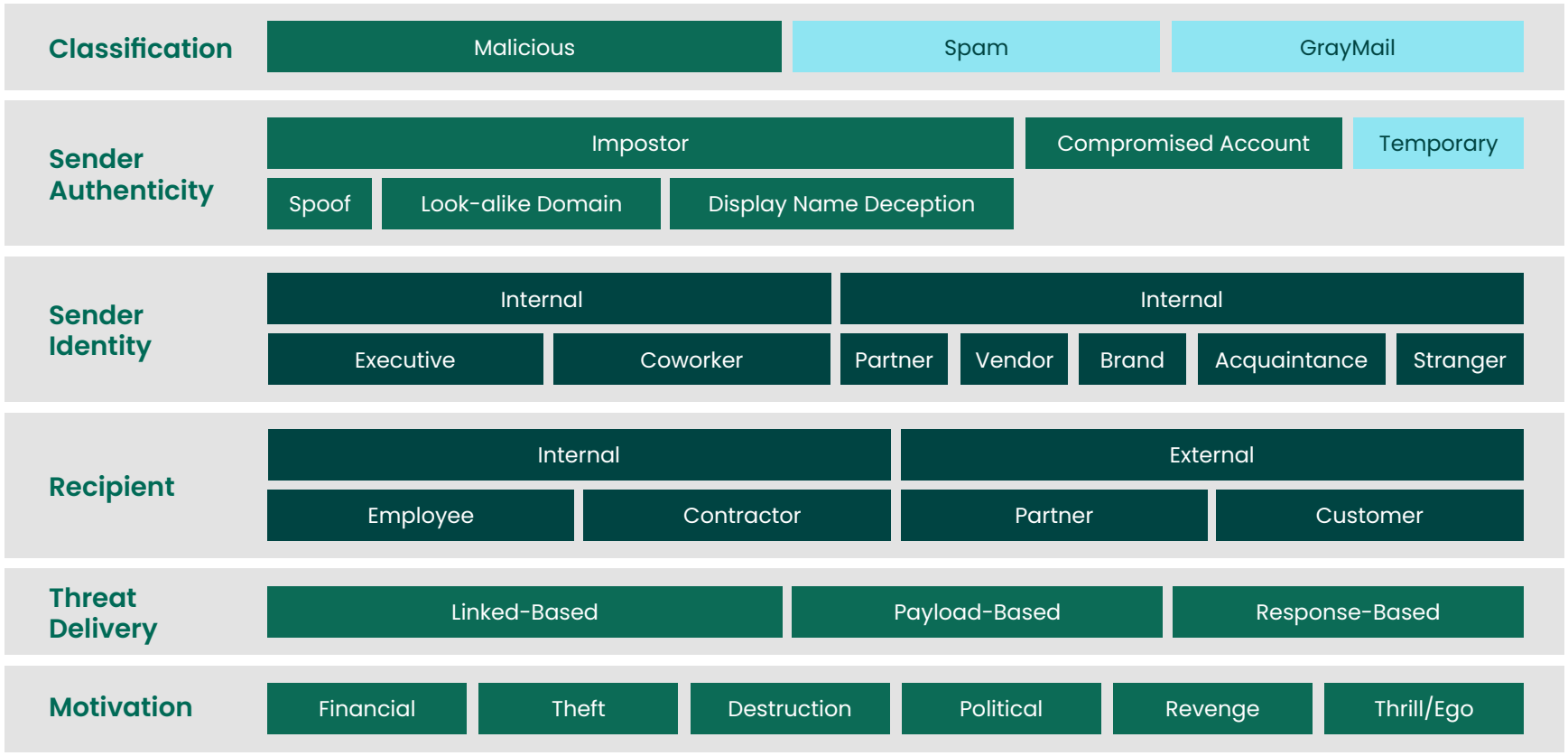
Leveraging applied data science and a diverse set of signals, Agari protects the workforce from inbound BEC scams, supply chain fraud, spear-phishing, and account takeover-based attacks—reducing business risk and instilling or restoring trust to your inbox. Agari also prevents spoofing of outbound email from the enterprise to customers, increasing deliverability and preserving brand integrity and reputation.

Learn more at **www.www.agari.com/products/dmarc-protection**.

About This Report

Taxonomy of Advanced Email Threats

ACID has established a classification system for cyber threats—a threat taxonomy—that breaks down common email-based attacks in terms of how they are carried out and what the perpetrators aim to achieve. This taxonomy helps readers understand the terms used in this report and what they mean to email security.



ACID Taxonomy of Advanced Email Threats

About This Report

Global DMARC Domain Analysis

With real-time statistics from the domains of top banks, social networks, healthcare providers, major government agencies and thousands of other organizations, the Agari Email Threat Center is the largest set of detailed DMARC data in the world both in terms of email volume and domains.

For broader insight into DMARC policies beyond what we observed in email traffic targeting Agari's customer base, we analyzed hundreds of millions of domains keeping in mind that in any given period, a rising number of new domains can cause changes to the total percentage of domains with DMARC policies and/or those at full enforcement, which is the level needed to prevent domains from being used to send phishing attacks.

Data in our 2022 report also includes DMARC adoption across key industry verticals pulled from public DNS records for primary corporate website domains of large companies with revenues above $1 billion USD. It is important to note that every vertical has shown incremental improvements in the percentage of their DMARC-enabled domains at p=reject since our last report in H1 2021.

End Notes

[1] Julia Gulevich, "Email Spoofing Attacks in 2022," Glock Apps, 2022

[2] Internet Crime Complaint Center (IC3), FBI's Center for Homeland Defense & Security, "Internet Crime Report 2021," March 22, 2022

[3] Kasey Panetta, "Gartner Top 10 Security Projects for 2020-2021," Gartner, September 15, 2020

[4] Chris Duckett, "DMARC inching its way onto Australian government domains," ZDNet, December 7, 2020

[5] Jeannine Balsiger, "State of Cybersecurity in Germany in 2021," Tripwire, December 7, 2021

[6] "Phishing attacks hit all-time high in December 2021," Help Net Security, March 3, 2022

[7] "STATISTICS ON REMOTE WORKERS THAT WILL SURPRISE YOU (2022)," Apollo Technical, January 16, 2022

[8] "Healthcare Data Leaks in 1st Half of 2021: Cases with More Than 10K Individuals Affected," Trend Micro™ News, July 28, 2021

FORTRA™

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-ag-gd-0323-r1-79d