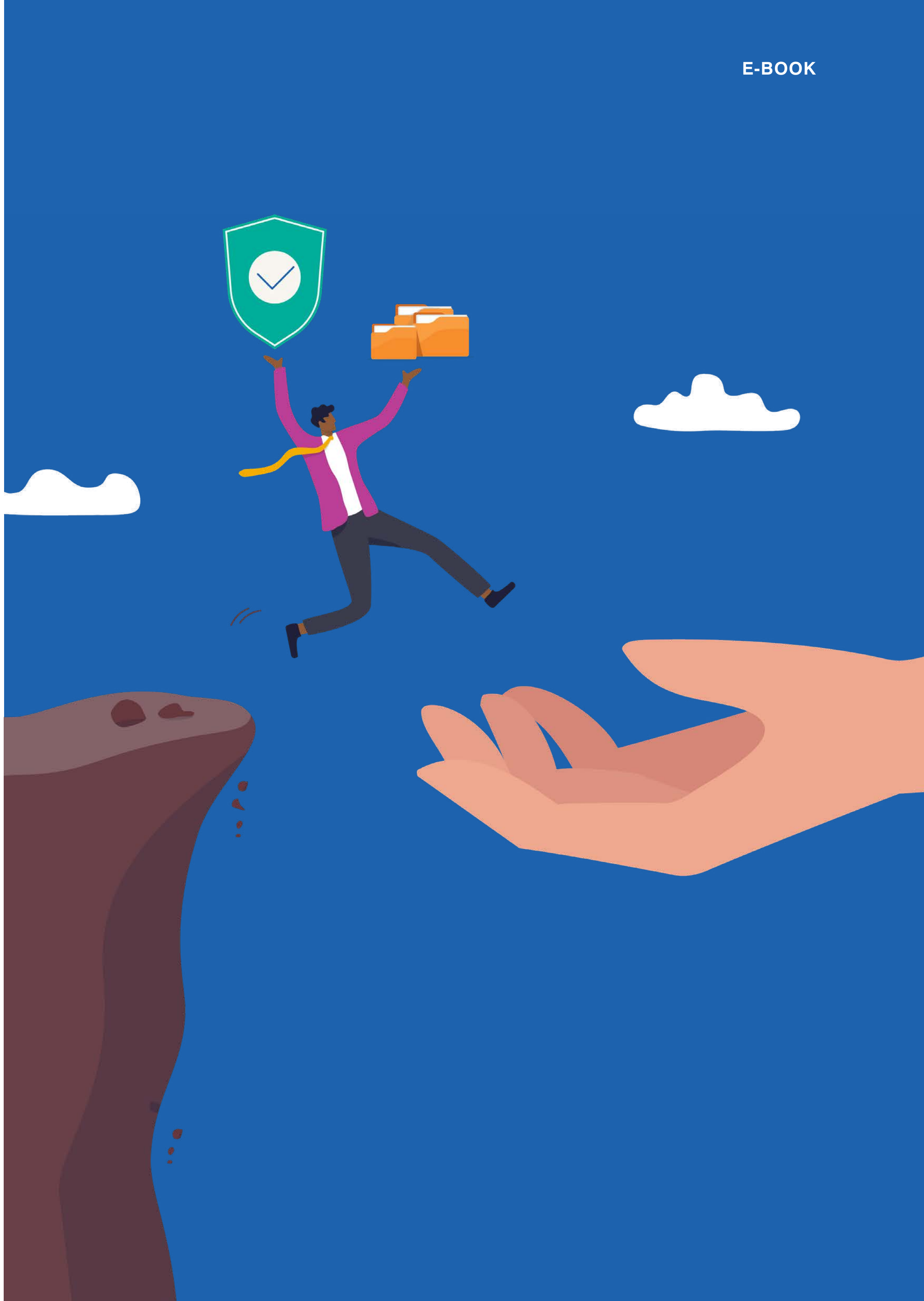
E-BOOK

Getting Started with DMARC

How email authentication can secure your email domain, prevent business email compromise and protect your brand



proofpoint.

Introduction

Email is great for business: it's inexpensive, scalable and, most important, effective at driving leads and revenue. Unfortunately, the very things that make email so popular—ease of use, convenience, transparency—also make it a vector of choice for cyber criminals.

Email fraud costs companies around the world billions and can destroy brand reputation and consumer trust in a matter of minutes. Highly targeted, low-volume business email compromise (BEC) scams are arguably the most dangerous, costing organizations around the globe $43 billion since 2016, according to the FBI.

[1] FBI. "Business Email Compromise: The $43 Billion Scam." May 2022.

$43 billion

is how much BEC has cost organizations around the globe since 2016
(Source: FBI)

$180,000

Is how much the average global BEC attack nets per incident
(Source: FBI)

12%

is the increase in organizations reporting phishing attacks in 2021 vs. the year before
(Source: Proofpoint)

86%

of organizations said they experienced phishing attacks in 2021
(Source: Proofpoint)

The Domain-based Message Authentication, Reporting and Conformance (DMARC) standard, unveiled by a group of leading email organizations in February 2012, is one of the most powerful and proactive weapons to date in the fight against phishing and spoofing.

It has reshaped the email fraud landscape, disrupting long-standing phishing strategies and forcing cyber criminals to abandon preferred targets. DMARC has the potential to nullify an entire class of fraud.

In this guide, we'll cover what DMARC is, how it works, its key benefits and why it should be a key part of how you protect your brand against BEC and a range of impostor threats.

[3] Proofpoint. "2021 State of the Phish." January 2021.
[4] Ibid.
[5] Verizon. "2021 Data Breach Investigations Report." July 2021.
[6] Chuck Brooks (Forbes). "Alarming Cybersecurity Stats: What You Need to Know for 2021." March 2021.

SECTION 1

What is DMARC?

Unveiled in 2012 by an industry consortium, DMARC is an open email authentication protocol that enables domain-level protection of the email channel.

Building on existing standards Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM), DMARC is the first and only widely deployed technology that can make the "header from" domain (what users see in their email clients) trustworthy.

Domain-based

Message

Authentication

Reporting and...

Conformance

Open email authentication standard

Launched in 2012

Founded by over 20 companies

DMARC allows email senders to

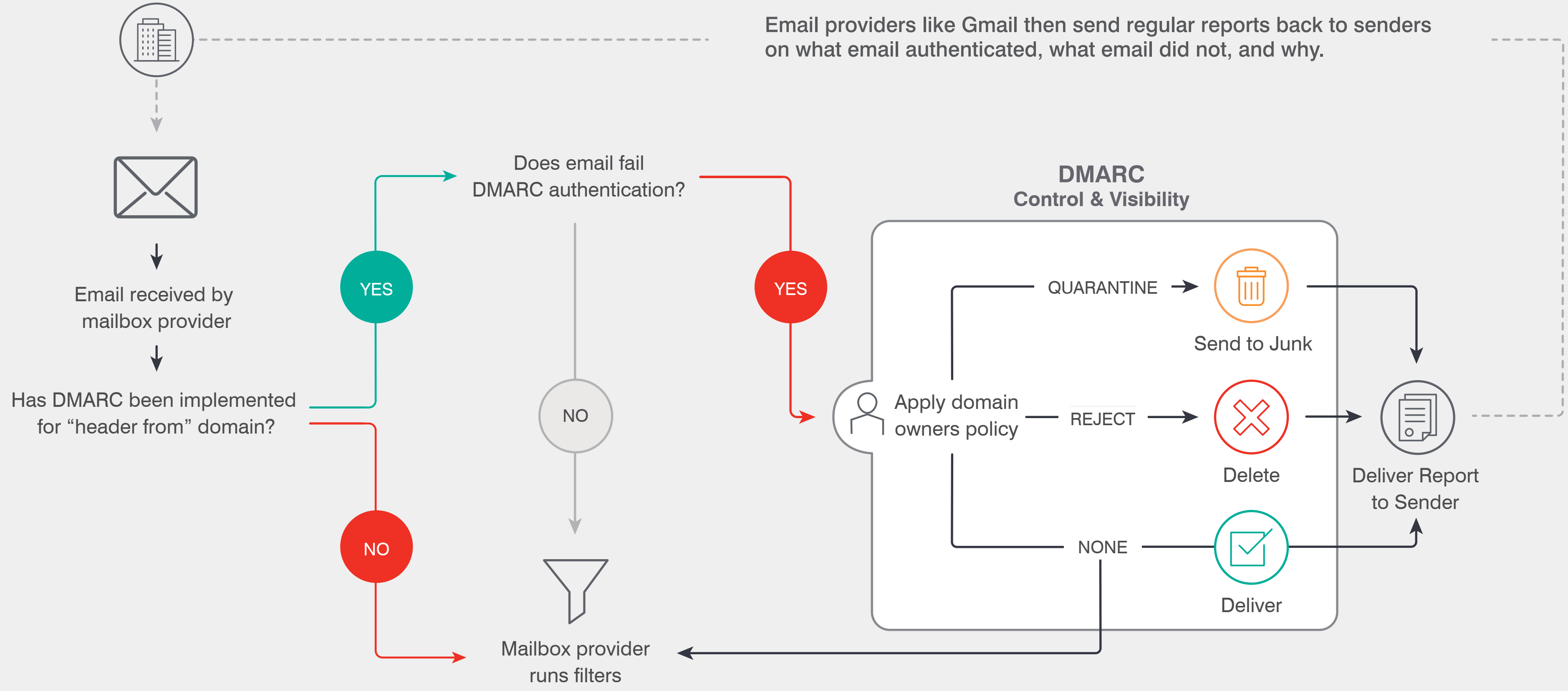
Reclaim control by authenticating legitimate email messages for their email-sending domains.

Instruct mailbox providers on how to treat messages that fail authentication, via an explicit policy setting. These messages can either be sent to a junk folder or rejected outright, protecting consumers from exposure to attacks.

Gain insights into the email threat landscape to help you identify threats against your customers and better protect your brand against phishing and spoofing.

SECTION 2

How DMARC Works


Email providers like Gmail then send regular reports back to senders on what email authenticated, what email did not, and why.
Email received by mailbox provider
Has DMARC been implemented for “header from” domain?
YES
NO
Does email fail DMARC authentication?
YES
NO
Mailbox provider runs filters
DMARC
Control & Visibility
Apply domain owners policy
QUARANTINE
Send to Junk
REJECT
Delete
NONE
Deliver
Deliver Report to Sender

DMARC Policy Settings

None: The entire email authentication ecosystem is monitored to map out legitimate traffic.

Quarantine: Messages that fail DMARC move to the spam folder.

Reject: Messages that fail DMARC do not get delivered at all.

SECTION 3

Why DMARC?

DMARC empowers senders to...

- Gain visibility into who is sending on your behalf, what email is authenticating, what email is not and why.
- Instruct email receivers on how to handle mail that does not pass authentication.
- Block phishing attacks spoofing owned domains before they reach employee and consumer inboxes.

DMARC empowers receivers to...

- Distinguish between legitimate senders and malicious senders.
- Foster consumer loyalty and employee protection.
- Improve and protect the reputation of the email channel.

> "Simply put, the DMARC standard works. In a blended approach to fight email fraud, DMARC represents the cornerstone of technical controls…to rebuild trust and retake the email channel for legitimate brands and consumers."
>
> **Edward Tucker,** Head of Cyber Security, HM Revenue & Customs

> "With stricter DMARC policies, users are safer, and the bad guys will be in a tough spot. More importantly, verified senders will unlock a massive wave of innovation and advancement for all our inboxes."
>
> **Jeff Bonforte,** SVP of Communications Products, Yahoo

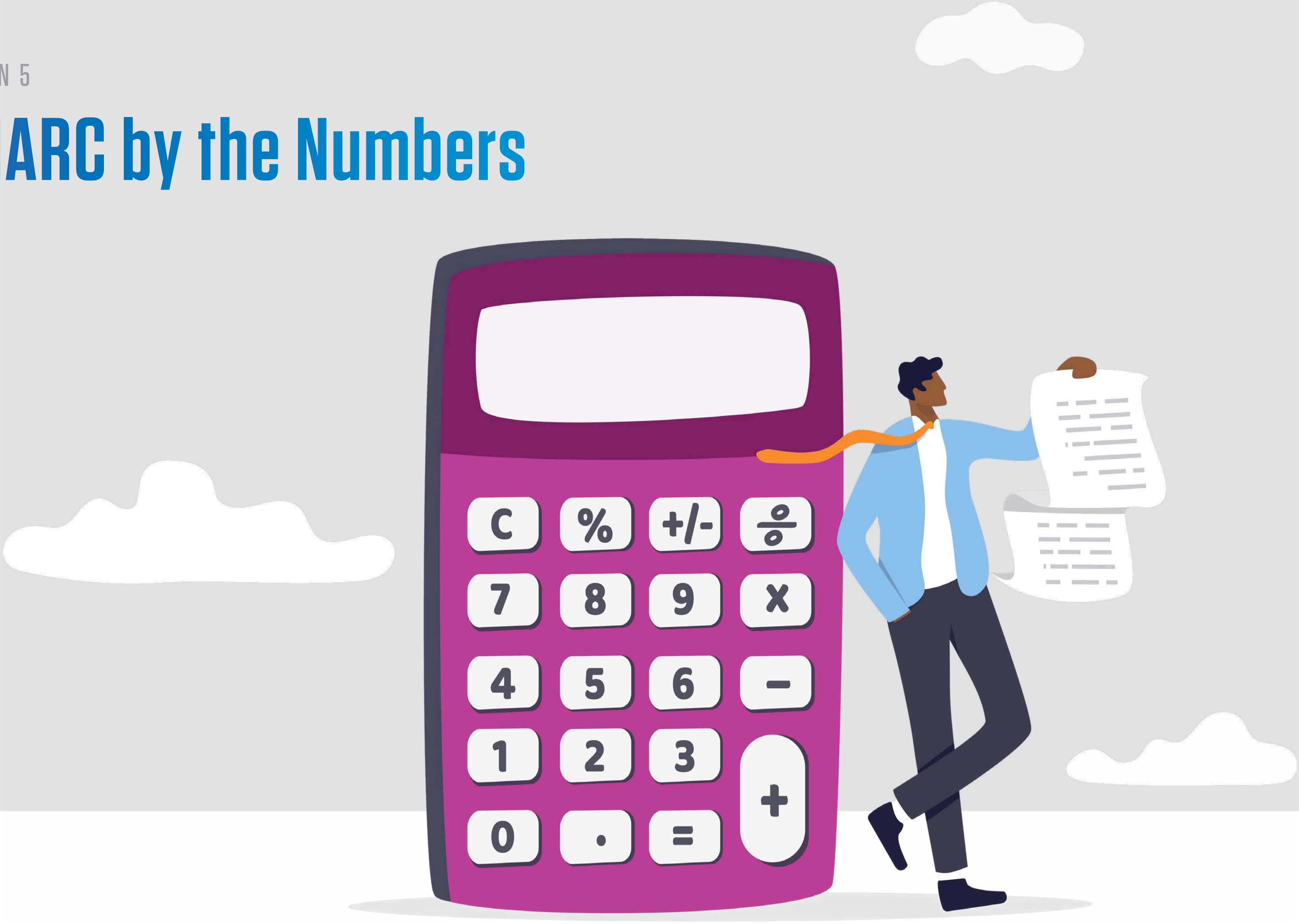
SECTION 4

The Benfits of DMARC

Protects employees, business partners, consumers and brands.	DMARC eliminates an entire class of fraudulent email before it reaches your employees, partners and customers.
Gives immediate insight into the email threat landscape.	You can’t control what you can’t see. Implementing DMARC gives you instant visibility into the threats targeting your company. It effectively shines a light on domain phishing and spoofing attacks that put your customers and brand reputation at risk.
Increases email deliverability and engagement.	Approximately one in five phishing attacks results in reduced deliverability and one in three results in reduced email engagement. DMARC increases both deliverability and engagement of legitimate email programs.
Reduces customer service costs.	By blocking phishing attacks, DMARC dramatically reduces customer service costs. Scandinavian retailer Blocket saw a 70% drop in customer-service tickets after implementing DMARC.
Reduces phishing remediation costs.	Phishing costs brands $4.5 billion every year. DMARC reduces the spend on fraud, reimbursement and phishing remediation costs.

SECTION 5

DMARC by the Numbers

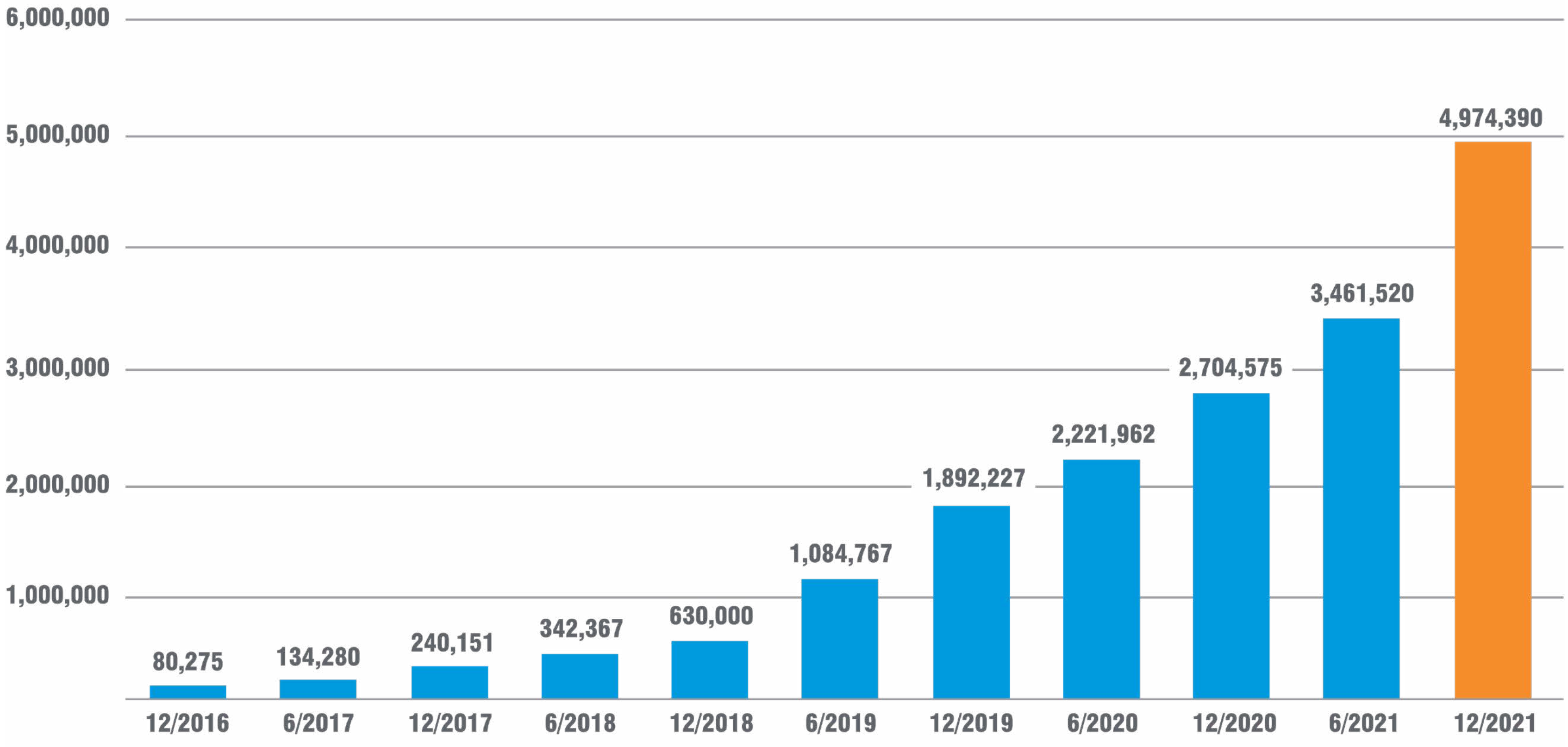


5 Million
unique DMARC records are active (as of December 2021)

65%
of the Global 2000 organizations have adopted DMARC authentication

26%
of the Global 2000 organizations have implemented a DMARC reject policy

Valid DMARC Records Confirmed via DNS



Source: DMARC.org

SECTION 6

Email Authentication at a Glance

DMARC is built on the backbone of two other important email authentication standards, SPF and DKIM. To fully understand DMARC, you must also understand the benefits of SPF and DKIM—and where they fall short.

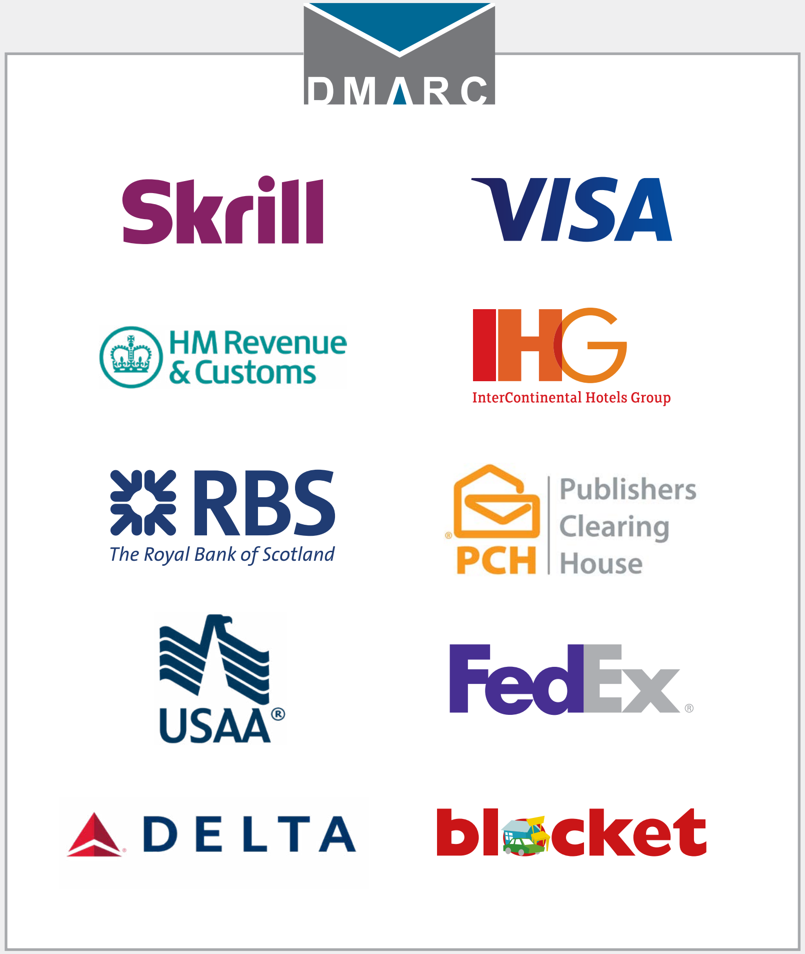
	SPF (Sender Policy Framework) www.open-spf.org	DKIM (DomainKeys Identified Mail) www.dkim.org	DMARC (Domain-based Message Authentication Reporting & Conformance) www.dmarc.org
Benefits	SPF allows brands to specify who can send email on behalf of their domain. Brands list the IP addresses of authorized senders in a DNS record. If the IP address sending email on behalf of the brand isn't listed in that SPF record, the message fails SPF authentication.	DKIM allows an organization to take responsibility for transmitting a message in a way that can be verified by the email provider. This verification is made possible through cryptographic authentication within the digital signature of the email.	DMARC ensures that legitimate email is properly authenticating against established DKIM and SPF standards. It also makes sure that fraudulent activity appearing to come from domains under a brand's control is blocked before ever reaching the customer's inbox.
Example DNS Record	v=spf1 ip4:204.200.197.197 -all	v=DKIM1; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDfl0chtL4siFYCrSPxw43fqc4zOo3N	v=DMARC1; p=reject; fo=1; rua=mailto:dmarc_agg@auth.yourdomain.com;ruf=mailto:dmarc_afrf@auth.yourdomain.com
Failings	• Keeping SPF records updated as brands change service providers and add mail streams is difficult. • Just because a message fails SPF, doesn't mean it will always be blocked from the inbox. • SPF breaks when a message is forwarded. • SPF does nothing to protect brands against cyber criminals who spoof the Display Name or "header from" address in their message.	• DKIM is more difficult to implement, thus fewer senders adopt it. • This spotty adoption means that the absence of a DKIM signature does not necessarily indicate the email is fraudulent. • DKIM alone is not a universally reliable way of authenticating the identity of a sender. • The DKIM domain is not visible to the non-technical end user, and does nothing to prevent the spoofing of the visible "header from" domain.	• While essential, DMARC is not a complete solution. • DMARC only protects your brand from 30 percent of email attacks (direct domain threats). • DMARC does not protect against brand spoofing (including Display Name spoofing and look alike domains).

SECTION 7

DMARC Champions: Brands

These DMARC champions have paved the way for the standard. These early adopters are at the forefront of the fight against email fraud and are proactively defending their customers against cyber criminals.

> “More and more companies have been adopting DMARC and email authentication over the past few years, with more vendors and service providers adding the necessary support to their offerings in order to make that adoption simpler.”
>
> **Steven Jones,** DMARC.org

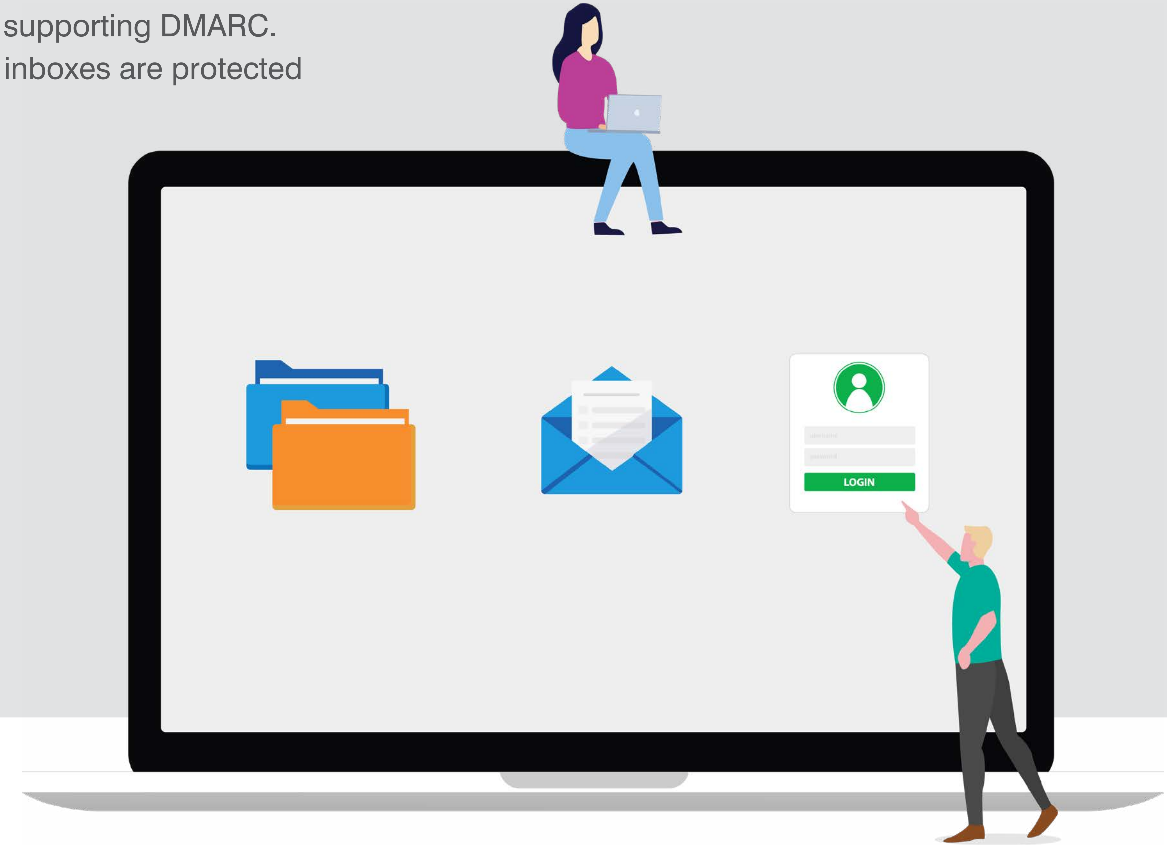

DMARC
Skrill
VISA
HM Revenue & Customs
IHG
InterContinental Hotels Group
RBS
The Royal Bank of Scotland
PCH
Publishers Clearing House
USAA
FedEx
DELTA
blocket

> “After we implemented a DMARC reject policy, we saw phishing customer service tickets drop by more than 70% which meant that service staff were able to focus on assisting customers with revenue generating inquiries.”
>
> Thomas Bäcker,
> Head of Customer Security,
> Blocket

SECTION 8

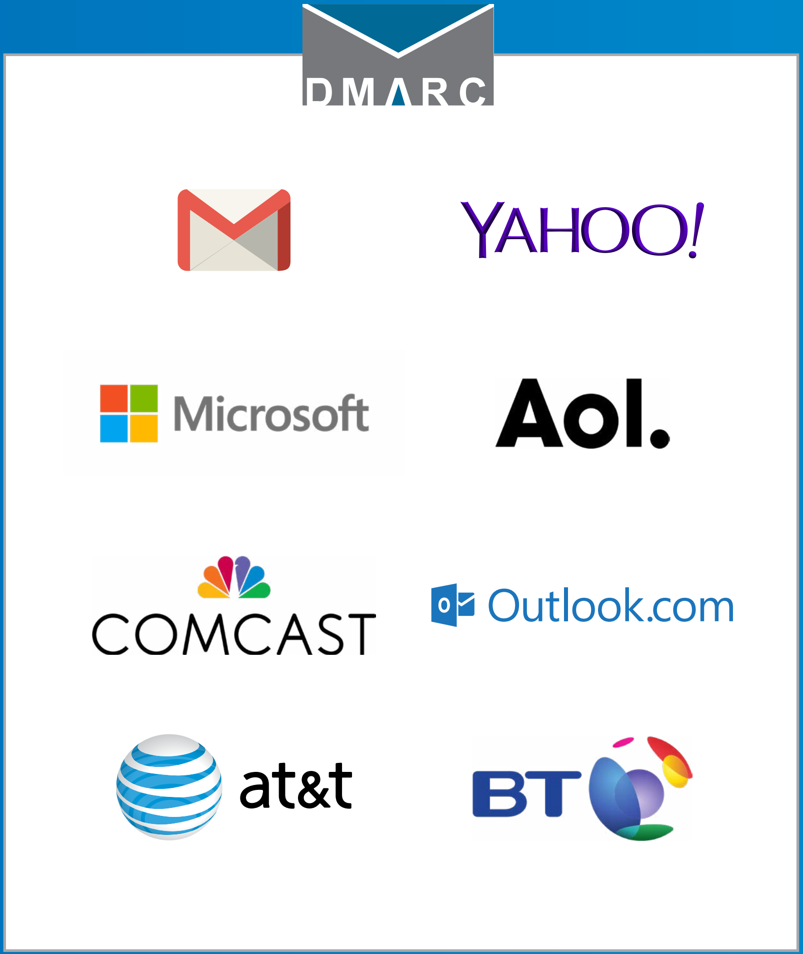
DMARC Champions: Mailbox Providers

Some of the world's largest mailbox providers are supporting DMARC. Today, an estimated 80% of the world's consumer inboxes are protected by DMARC.



> “We’re rapidly moving toward a world where all email is authenticated. Implementing a DMARC policy ensures that a sender’s reputation doesn’t drop due to the actions of spammers. If your domain doesn’t protect itself with DMARC, you will be increasingly likely to see your messages sent directly to a spam folder or even rejected.”

John Rae-Grant,
Product Manager, Google



> “Overnight, the bad guys who have used email spoofing to forge emails and launch phishing attempts pretending to come from a Yahoo! Mail account were nearly stopped in their tracks.”

Jeff Bonforte,
SVP of Communications Products, Yahoo

SECTION 9

DMARC Tag Glossary

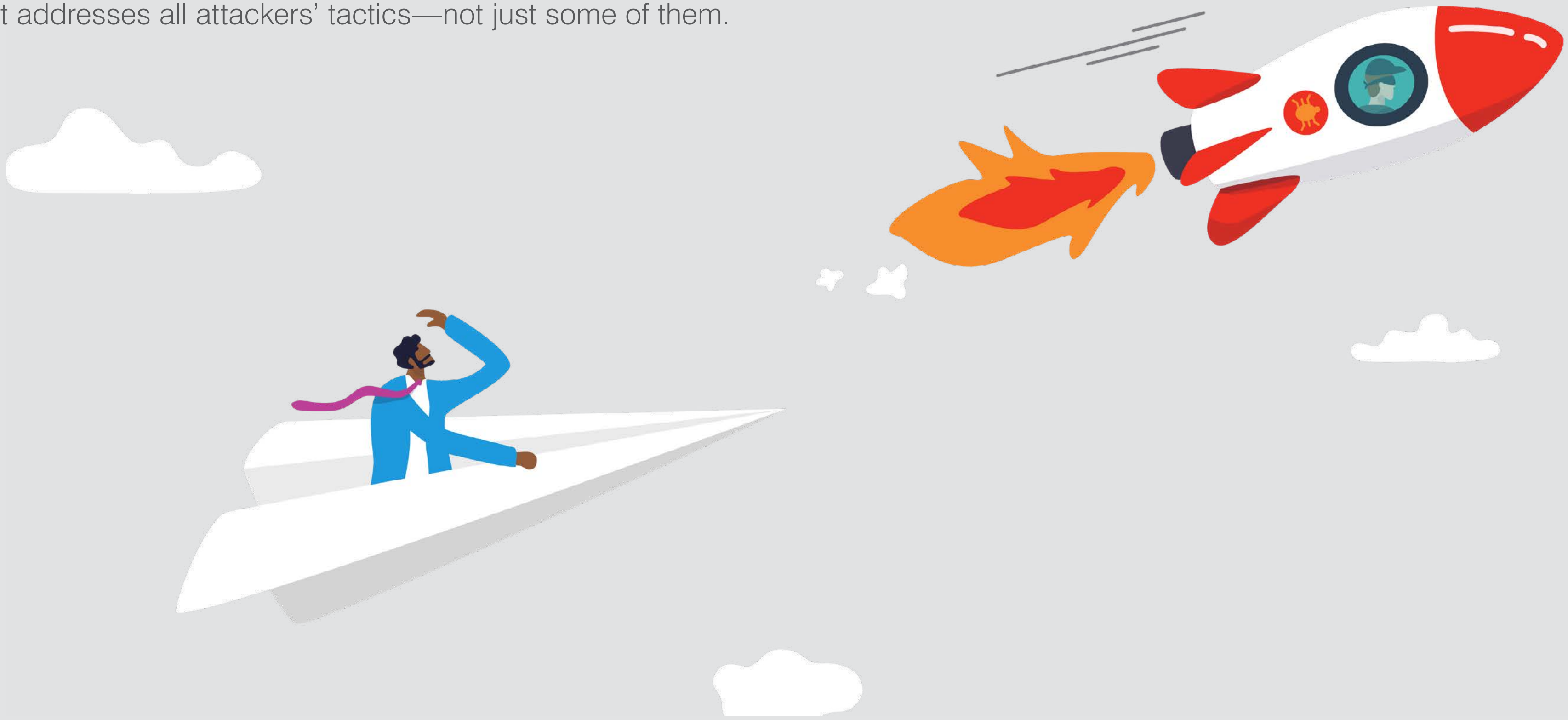
Tag Name	Purpose	Sample
v	Protocol version	v=DMARC1
p	Policy for domain	p=quarantine
pct*	% of messages subjected to filtering	pct=20
rua*	Reporting Uniform Resource Identifier (URI) of aggregate reports	rua=mailto:aggrep@example.com
sp*	Policy for subdomains of the domain	sp=reject
aspf*	Alignment mode for SPF (strict or relaxed)	aspf=r
ruf*	Reporting URI of forensic reports	ruf=mailto:aggrep@example.com
adkim*	Alignment for DKIM (strict or relaxed)	adkim=r
ri*	The number of seconds elapsed between sending aggregate reports to sender.	ri=86400
fo*	Provides options for generation of failure reports.	“fo=1”

*Optional

SECTION 9

Time to Start Your DMARC Journey

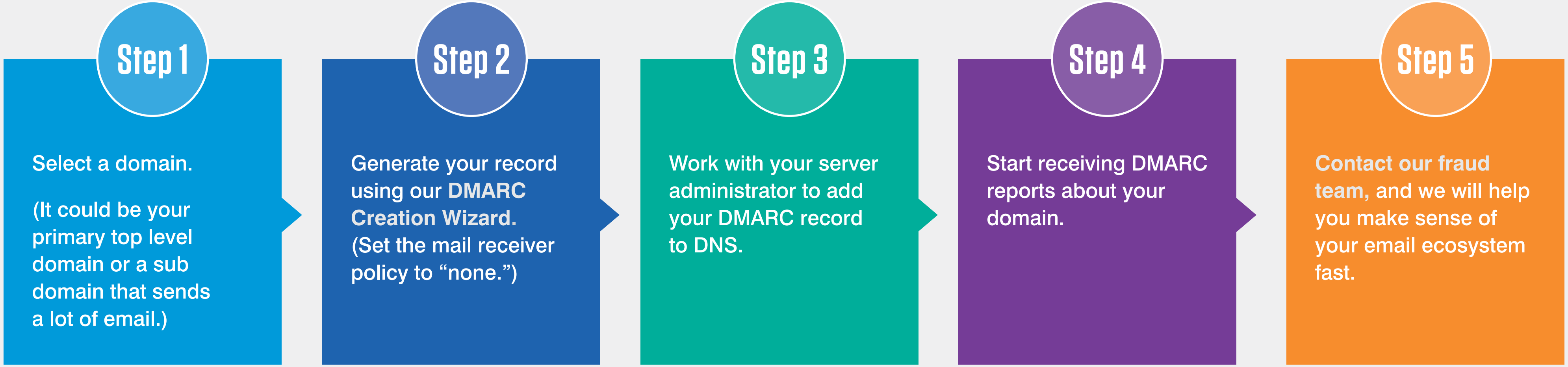
BEC attacks are complex and multifaceted. That’s why they require a complete solution that addresses all attackers’ tactics—not just some of them.



While there's no silver bullet for BEC and EAC, deploying DMARC is a good start. It's a critical component in defending against impostor threats, especially those that spoof trusted email domains. DMARC is the most effective way to protect against domain spoofing and stopping fraudulent emails from using your domain.

At Proofpoint, we help some of the world's largest brands successfully deploy DMARC. And while every organization is unique, most follow these steps toward full deployment over time.

It starts with a very simple first step: create a DMARC record in DNS and shine a light onto your entire email ecosystem.



Step 1

Select a domain.

(It could be your primary top level domain or a sub domain that sends a lot of email.)

Step 2

Generate your record using our **DMARC Creation Wizard.** (Set the mail receiver policy to "none.")

Step 3

Work with your server administrator to add your DMARC record to DNS.

Step 4

Start receiving DMARC reports about your domain.

Step 5

Contact our fraud team, and we will help you make sense of your email ecosystem fast.

Congratulations. You have taken your first steps to fighting email fraud.

To learn more about how Proofpoint can help you effectively combat BEC attacks and protect your brand, visit **proofpoint.com**.

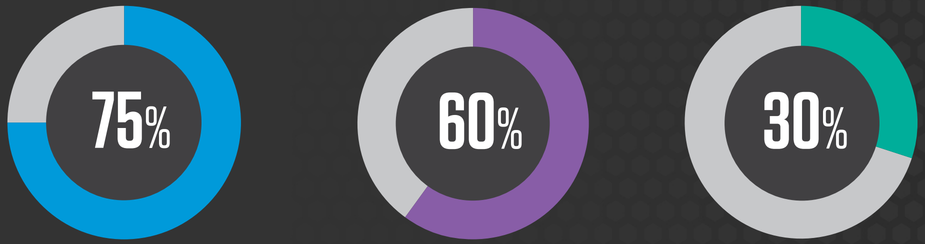
About Proofpoint

The Proofpoint Nexus Threat Graph blends the industry's best security research, technology and threat data to keep you protected at every stage of the attack lifecycle. No one else has better insight into how today's cyber attacks target people.

Every day, we analyze more than:

2.6B EMAILS	**49B** URLS	**1.9B** ATTACHMENTS
1.7B MOBILE MESSAGES	**430M** WEB DOMAINS	**143,000** SOCIAL MEDIA ACCOUNTS

We are trusted by more than:



OF THE FORTUNE 100

OF THE FORTUNE 1000

OF THE FORTUNE GLOBAL 2000

8,000 ENTERPRISES

200,000 SMALL BUSINESSES

LEARN MORE

For more information, visit proofpoint.com.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at www.proofpoint.com.