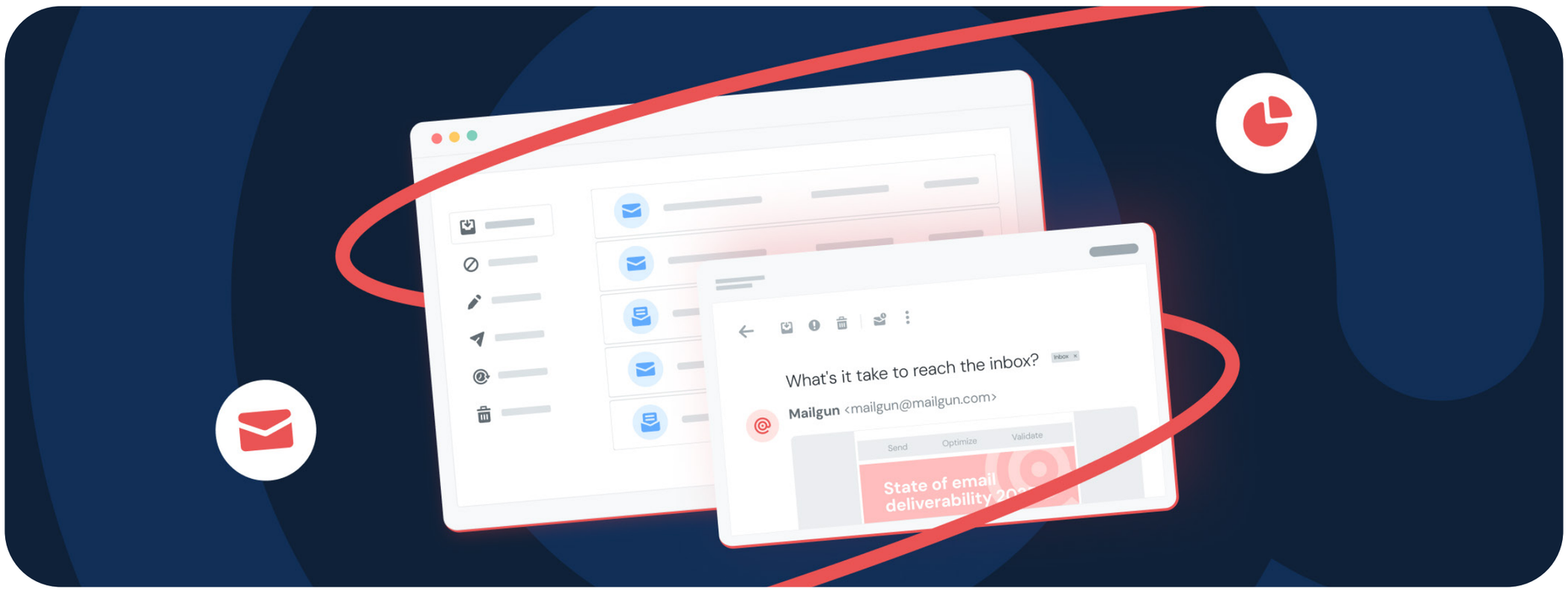
SINCH Mailgun

State of email deliverability 2025

The changes and challenges of reaching the inbox

Table of content



INTRODUCTION

State of email deliverability 2025

Imagine what would happen if your organization's emails suddenly stopped reaching your customers and prospects. If that thought made your heart skip a beat, you already understand the importance of email deliverability. Email is an indispensable connection point, which should make achieving inbox placement a priority. But is it?

For the second time in two years, Sinch Mailgun surveyed senders across the globe to find out more about their challenges, common practices, and where they may have misconceptions about email deliverability. Use these findings and the helpful feedback from industry leaders to make sure your messages land in the inbox.

The evolution of email deliverability

Sometimes change happens slowly. Other times, there's an evolutionary leap, and you've got to adapt to survive and thrive. We can't talk about the state of email deliverability without mentioning the **new sender requirements** from major mailbox providers Gmail and Yahoo Mail in 2024.

These new rules caused concerns among certain senders. Some never even heard about the changes. Others remained confident their inbox placement rates would be fine. **50% of senders who were familiar with the new bulk sender requirements say they made changes to their email programs in 2024 to adapt.** Of course, that means many others didn't see the need to change anything.

Wondering if you missed something? No worries. We'll review what's new for email deliverability and point you in the right direction.

The truth is, senders who already understood what it takes to reach the inbox didn't have to change much. Most of the requirements were already considered best practices. Gmail and Yahoo simply tried to nudge everyone in the right direction. Senders who already worked to respect and protect their subscribers had very little to worry about.

> “The lesson here is that prioritizing deliverability, including aspects such as email authentication and compliant list building, is an excellent way to future-proof your email program. Do the right thing now if you truly want email to remain an effective channel.”

Kate Nowrouzi
VP of Deliverability and Product Strategy at Sinch

Key findings on the state email deliverability

This report is jam-packed with survey results from more than 1,000 people representing a wide variety of industries, job roles, and send volumes. The findings paint a picture of the state of email and some of the biggest challenges senders face. Here are just a few of the most notable:

78.5%
rate the importance of deliverability 8/10 or higher.

48%
say staying out of spam is a top challenge

53%
are not monitoring email blocklists for their sending domains and IPs.

39%
rarely or never conduct email list hygiene.

Email deliverability can be complex and confusing. Getting it right involves the attention and efforts of technical and marketing team members. The good news is, as you work to improve deliverability, you’ll also **improve the customer experience** as well as the positive impact email has on your organization’s communications.

CHAPTER 1

The year of Yahooglesoft

When a pair of tech powerhouses like Google and Yahoo **make an announcement** together, everyone tends to listen. That was the case in late 2023 when many senders learned they needed to meet stricter requirements to continue reaching Gmail and Yahoo Mail inboxes.

Like some sort of mailbox provider power couple, the requirements even earned a nickname. These so-called “Yahoogle” updates prompted plenty of email senders and platforms to make changes. But what was the point?

When the requirements first were released we polled senders on the Let’s find out why Yahoo and Google’s new requirements and asked if they matter and how they impacted senders’ behaviors and opinions.

Key findings on Yahoo and Gmail sender requirements

63%

of senders were at least somewhat familiar with the new requirements.

49.5%

of senders who were aware of the new requirements made changes to their email programs in response.

79%

of senders who made changes updated email authentication protocols.

64%

of senders believe the new requirements are necessary or good for the future of email.

Recapping the new sender requirements

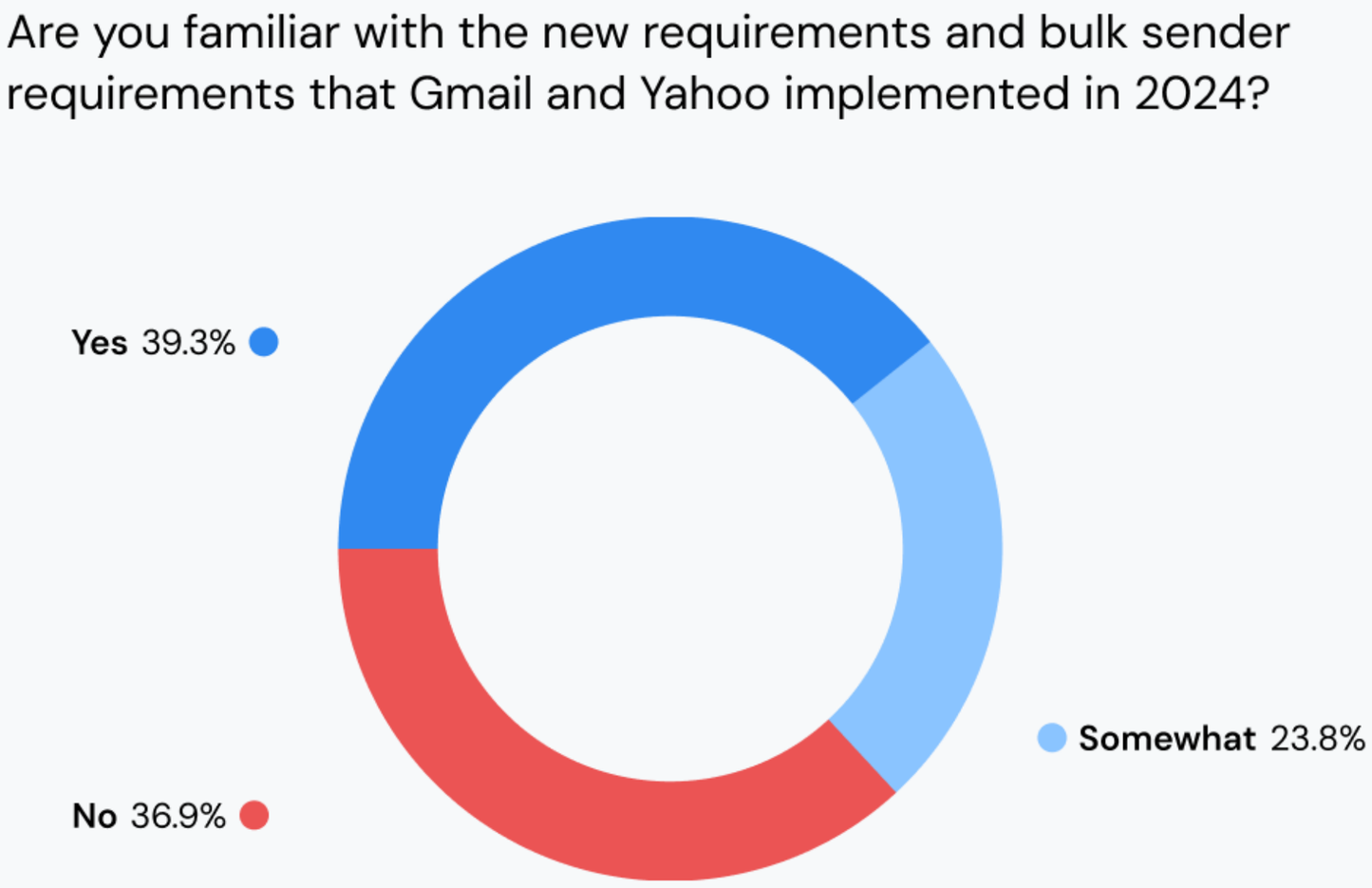
While Yahoogle felt like a big deal to some, there were others who never even got the news. For many with low email sending volumes, there wasn't much to update. **Gmail and Yahoo were mostly concerned with the practices of bulk email senders.** Google defines a bulk sender as anyone sending around 5,000 messages per day to personal Gmail accounts.

Don't get hung up on a specific number. According to Marcel Becker of Yahoo, any organization sending mass messages on a regular basis should consider itself a bulk sender

> "The number is not 5,000, or 6,000, or 4,000. If you send 4,999 messages, you still have to follow the requirements. If you're sending the same email to a lot of people, you're a bulk sender."

Marcel Becker
Senior Director of Product at Yahoo

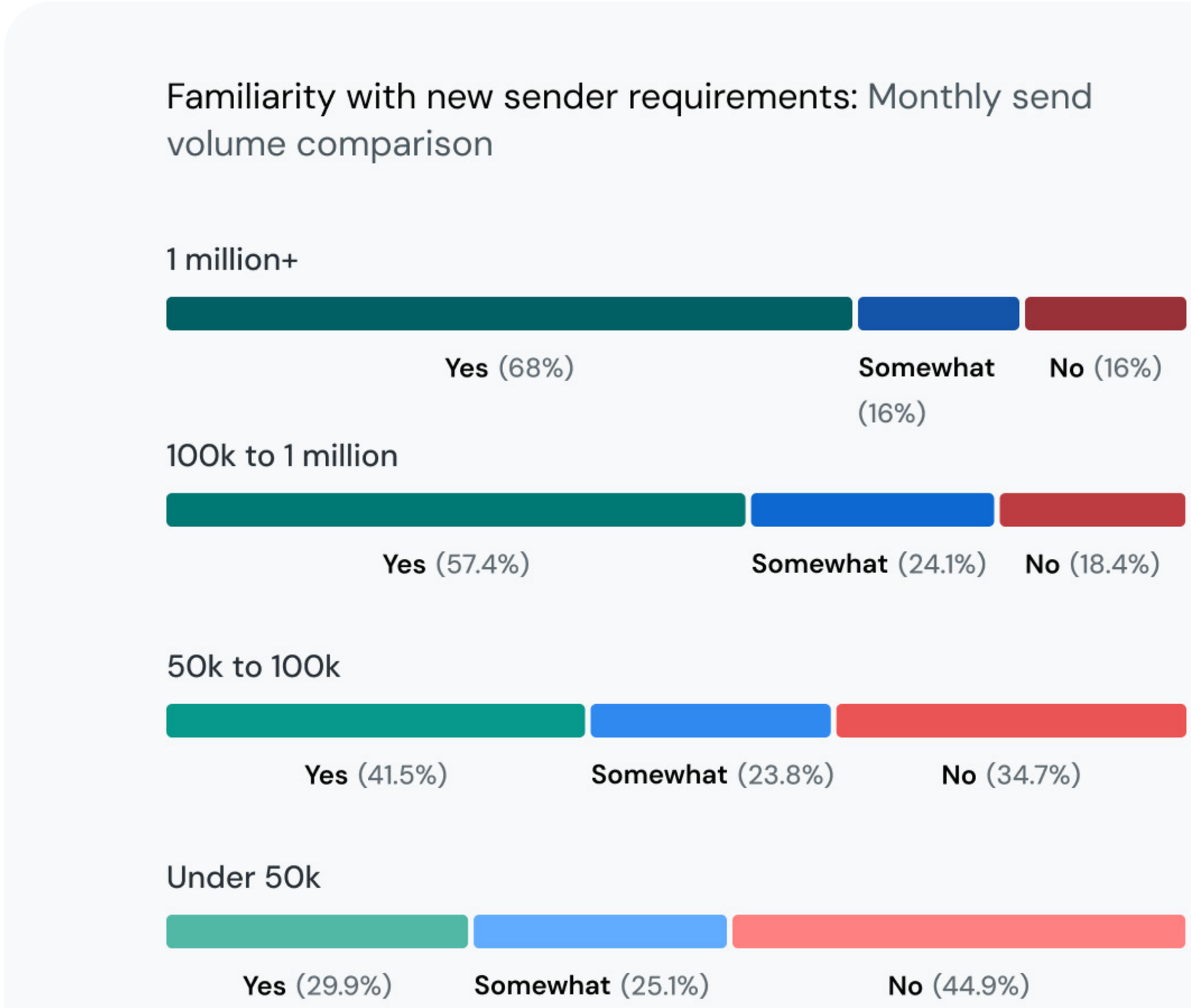
Our global survey found **63% of all senders were at least somewhat familiar with the new sender requirements from Google and Yahoo.**



While it's true that more than a third of our survey respondents hadn't heard of Yahoogle, the survey results show most bulk senders were aware of the updated requirements.

When we look at individual monthly send volumes, it's clear that high-volume senders were more familiar with the changes. 84% of senders with a monthly volume greater than one million emails per month were at least somewhat familiar. The same goes for 81.5% of senders with monthly volumes between 100,000 and one million.

Even among those with the lowest send volumes, more than half of respondents (55%) had at least heard about the Yahoo and Google requirements.



Sinch Mailgun's research also found that nearly half of all senders (49.5%) who knew about Yahoo and Google sender guideline updates made specific changes to their email programs in response. Those changes typically involved three things:

1. Implementing email authentication protocols (SPF, DKIM, and DMARC).
2. Enabling one-click unsubscribe functionality.
3. Maintaining spam complaint rates below a 0.3% threshold.

We'll briefly explain each of these updates here. You'll find more in **Sinch Mailgun's article on 2024 inbox protections**.

Changes to email authentication requirements

The biggest changes for most senders involved Google and Yahoo's requirements around **email authentication protocols.** That includes the following:

- Sender Policy Framework (SPF)
- DomainKeys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting and Conformance (DMARC)

Put simply, email authentication helps mailbox providers like Gmail and Yahoo verify sending domains and IP addresses as legitimate. Authentication protocols make it easier to stop **email spoofing**, which keeps potentially malicious messages from reaching inboxes.

Now all senders must use SPF or DKIM to authenticate their emails. However, the requirements are more specific for those sending mass email. Bulk senders must use both SPF and DKIM. Plus, they need to implement DMARC with a minimum policy of p=none.

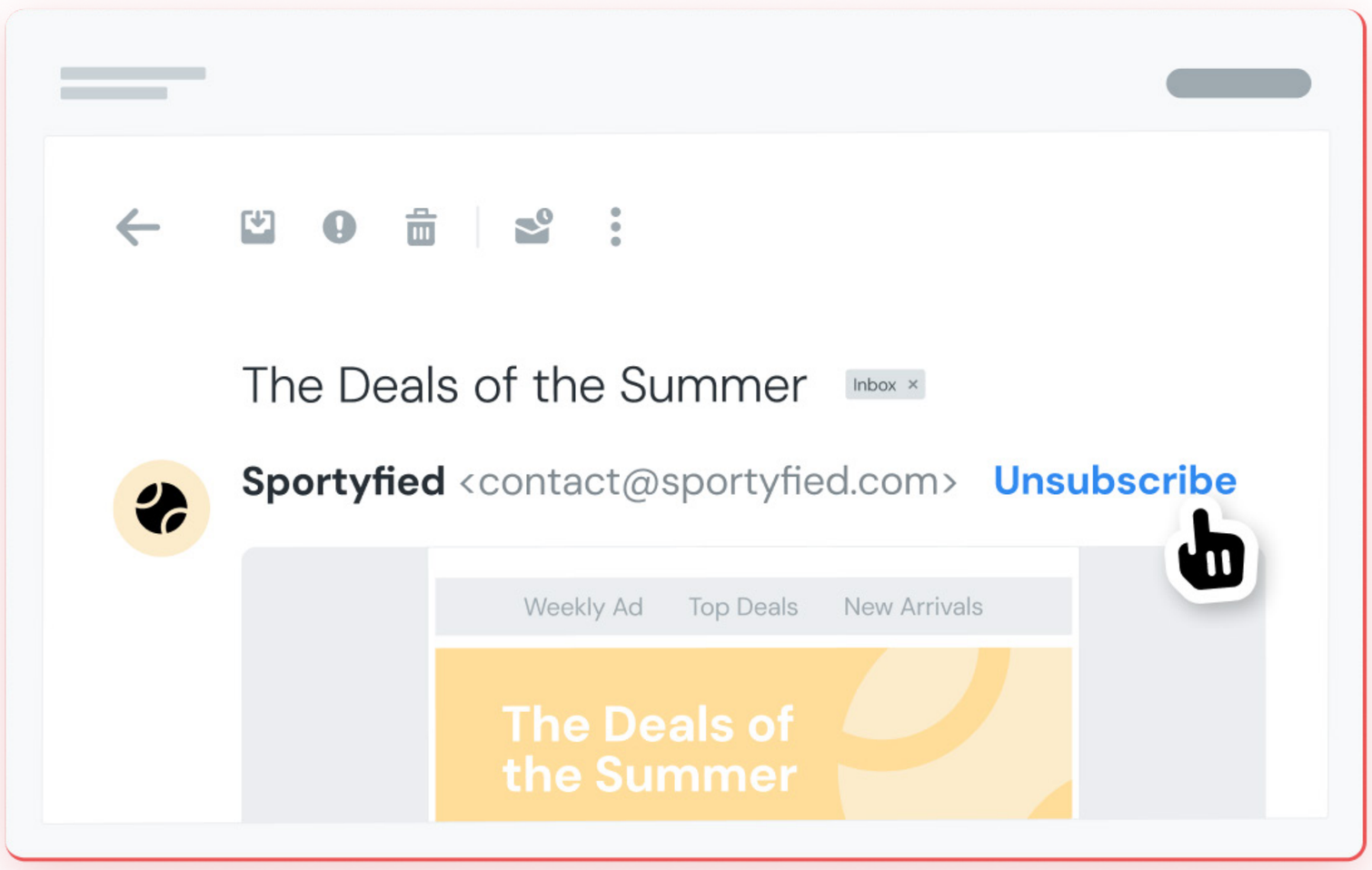
We'll dive deeper into email authentication in Chapter 2 of this report.

One-click unsubscribe with RFC 8058

Another important bulk email sender requirement involves making it easy for contacts to unsubscribe. **Gmail and Yahoo now require one-click unsubscribe functionality, and senders must follow through with those unsubscribe requests within two days.**

One-click unsubscribe is directly connected to **RFC 8058**, which involves the **List-Unsubscribe** and **List-Unsubscribe-Post** email header fields.

RFC 8058 is an email standard that lets recipients unsubscribe without visiting a preference center or taking any further action. In Gmail, one-click unsubscribe appears to users like this:



An email campaign with one-click unsubscribe.

With RFC 8058, recipients can easily unsubscribe from a brand's emails. This is obviously beneficial to recipients, but it also benefits the sender. **Making it easy to unsubscribe makes it less likely you'll get user-generated spam complaints.**

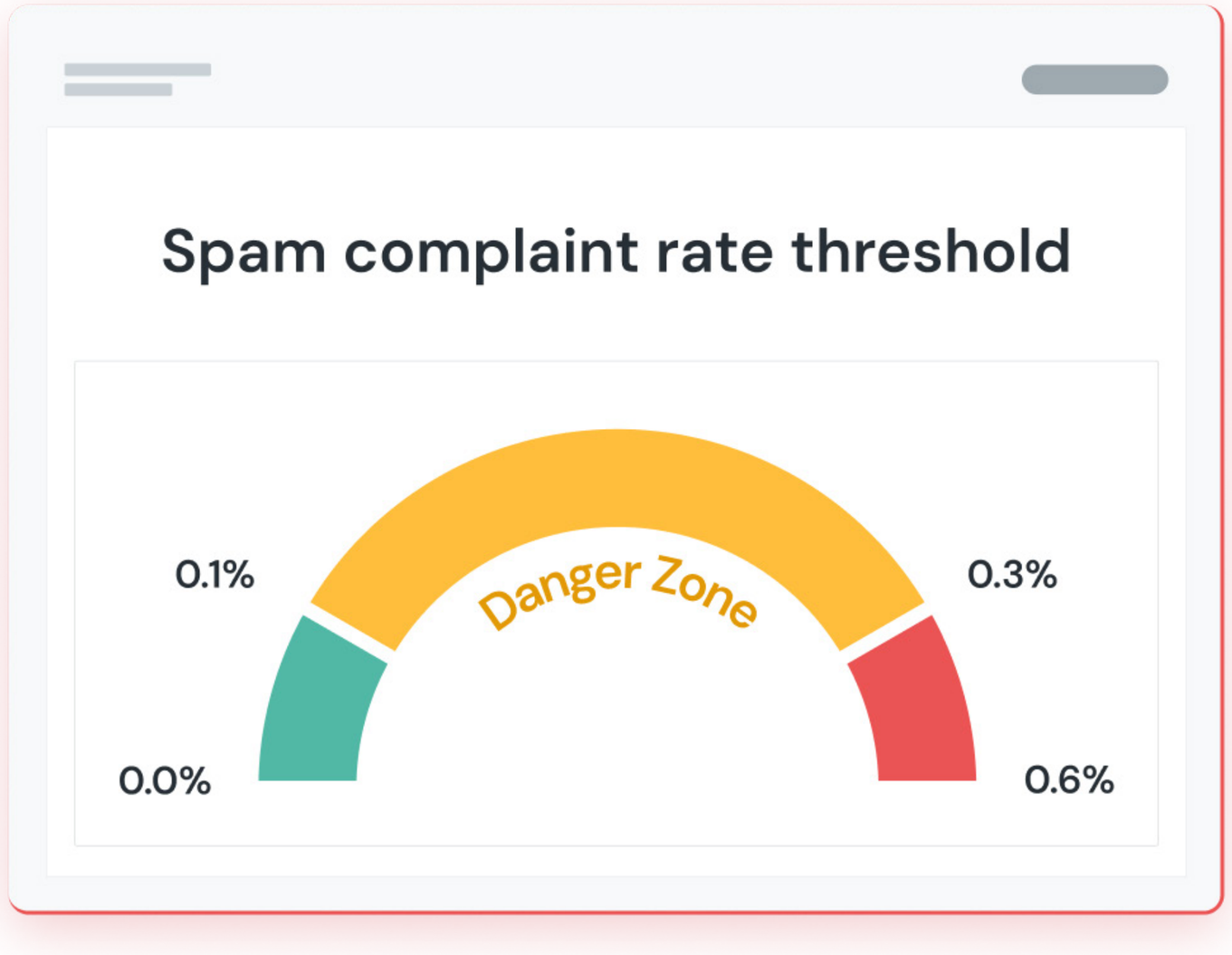
An advantage for Sinch Mailgun users is that we can automatically implement one-click unsubscribe for you, inserting the necessary headers and processing requests to be removed from your list. Learn more about **unsubscribe handling and links.**

Spam complaint thresholds

Let's get something straight about how recipients perceive spam... **People complain about spam when emails are unwanted or intrusive.** Even though you may have properly obtained consent, subscribers still choose to mark emails as spam if they are annoyed or it's hard to unsubscribe.

Yahoo and Google sender requirements in 2024 stipulate a 0.3% threshold for the **spam complaint rate**. However, it is strongly suggested that bulk senders keep their spam complaint rate below 0.1% without ever reaching the 0.3% threshold.

What this means is once your spam complaint rate exceeds 0.1%, you're entering a "danger zone." If the complaint rate reaches 0.3%, you're in real trouble. That's when you're at **risk of being blocklisted.**



Here's how the spam complaint rate is calculated:

```
Number of complaints / Number of emails received X 100 = Spam complaint rate %
```

It only takes one complaint out of 1,000 messages for a 0.1% spam rate. So, if you send 1,000 emails and get just three complaints, you've already hit the 0.3% threshold.

This may seem intense. But Yahoo's Marcel Becker says this has been the policy of many mailbox providers for quite some time

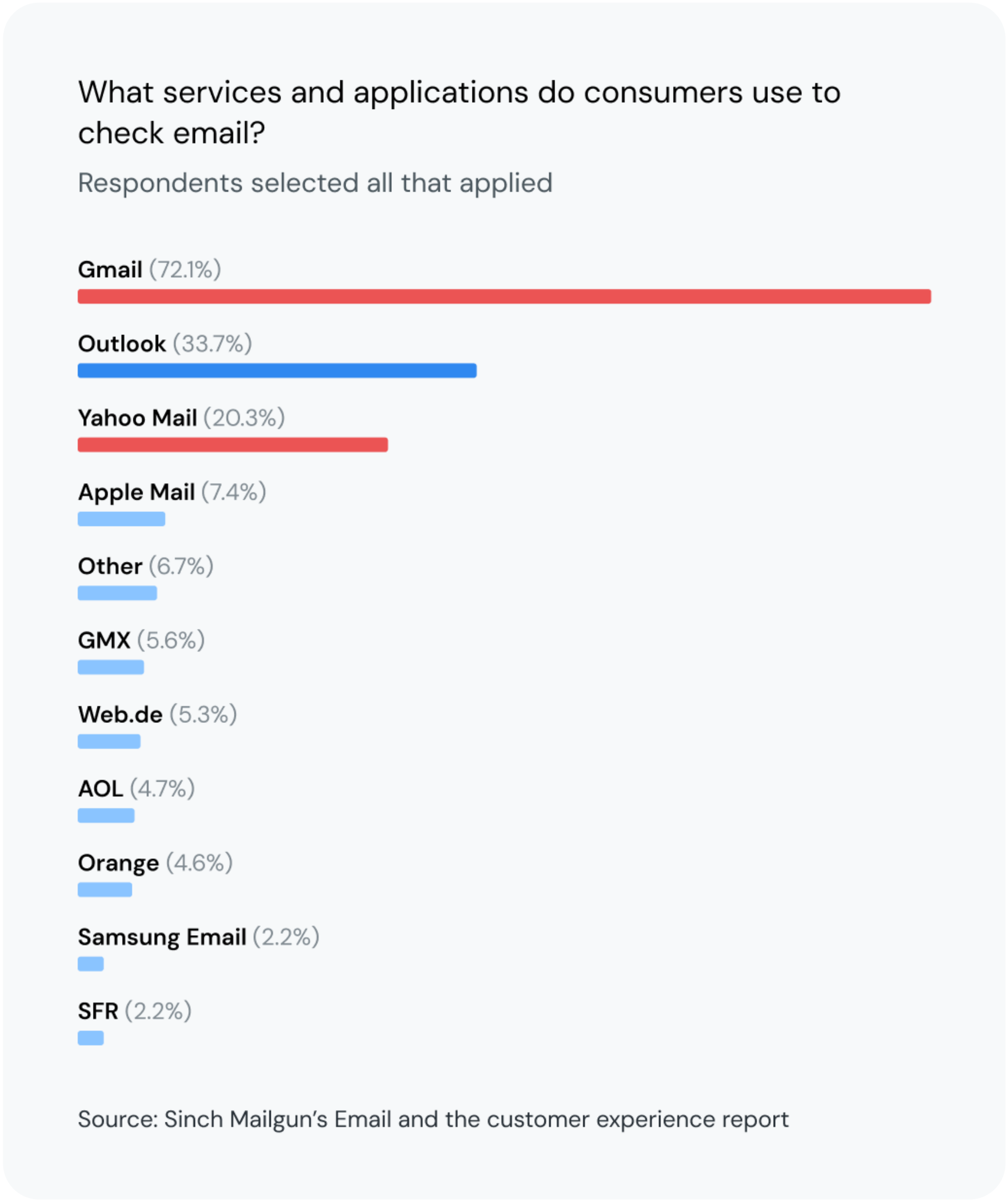
> “This is nothing new. We have always looked at these spam rates and there are other companies out there also using 0.3%... If you’re a good sender, your spam rates will be well below 0.3%.”

Marcel Becker
Senior Director of Product at Yahoo

How did senders respond to the new requirements?

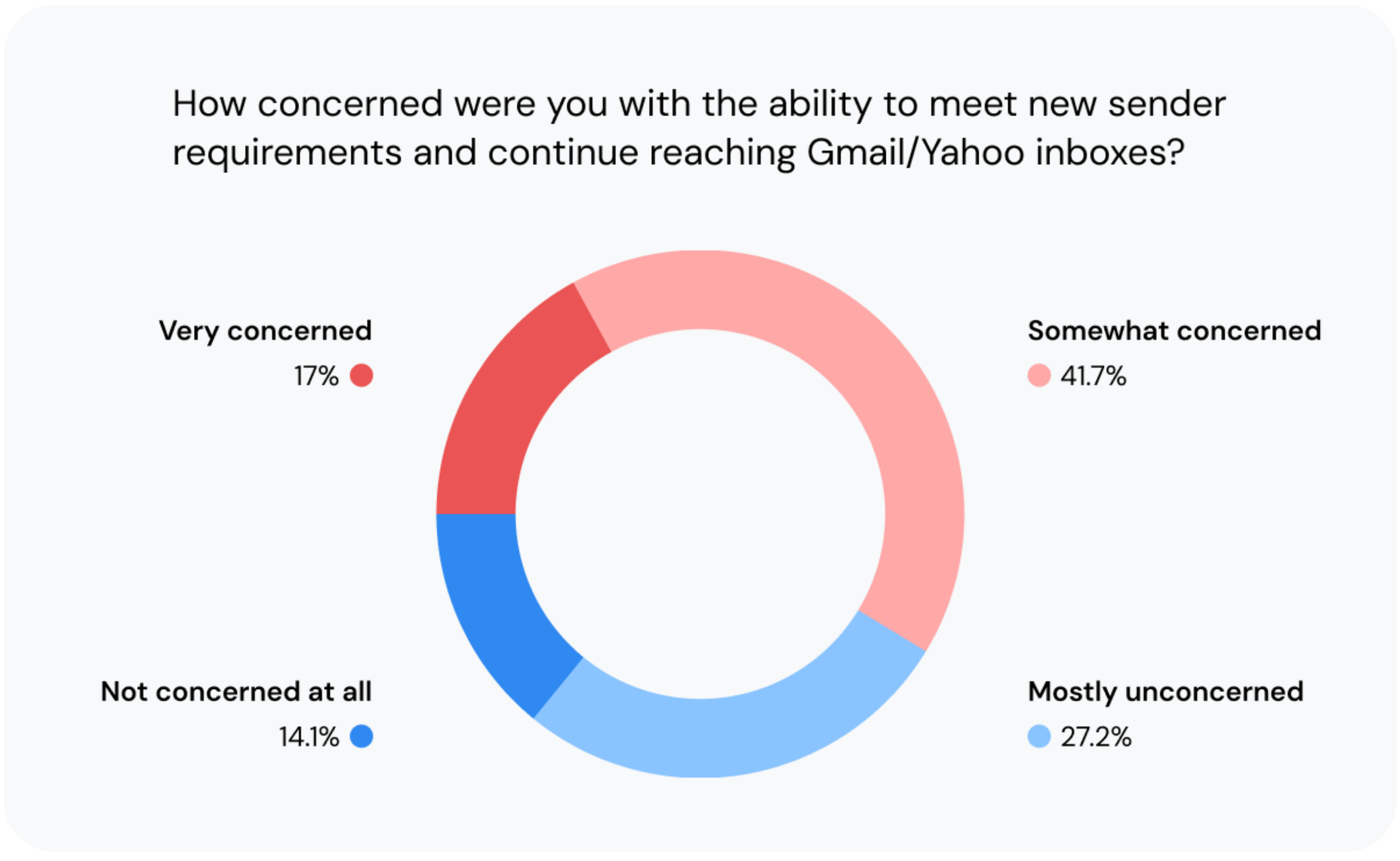
The truth is, many of the new sender requirements from Google and Yahoo weren’t much more than best practices that companies should’ve been following already. That’s why not everyone was worried or needed to make changes to their email programs in 2024.

There is, however, a good reason that businesses would be concerned with being unable to reach personal Gmail accounts. When Sinch Mailgun surveyed global consumers for the **Email and the customer experience** report, we found that more than 72% of respondents used Gmail. Yahoo Mail took the third most popular spot with just over 20% saying they use the service.



Consumer survey results from "Email and the customer experience"

Seeing how prevalent Gmail and Yahoo are among consumers, it was no surprise to see how senders responded when we asked them about their level of concern over the requirements. Close to 42% were somewhat concerned while 17% were very concerned. About 14% of senders in our survey were not concerned at all. 27% were mostly unconcerned. That reflects an approximate 60/40 split between those who were worried and those who weren't.



Send volumes seemed to make little difference. However, senders in the middle of the pack did have slightly higher levels of concern. 21% of the two groups with monthly send volumes between 50,000 and 1-million emails per month said they were **very concerned** about meeting the new requirements.

While 59% of respondents were concerned about the new sender requirements, only 23% reported having any email deliverability challenges after Gmail and Yahoo began enforcing them.

What did senders change to meet requirements?

Among the senders who were aware of Yahoo and Google's new sender requirements for 2024, **49.5% made specific changes to their email programs.** In some cases, that involved complying with the stricter rules. Many others adjusted their programs to avoid trouble with spam complaints.

By far, updates to email authentication were the most common change. **Almost 80% of senders who made changes updated authentication practices due to Yahoogle.**

About a third of senders (33.1%) took steps to ensure they were implementing RFC 8058 for one-click unsubscribe. **37% of senders who made changes began to closely monitor their spam complaint rate.** Many of the other changes are also connected to avoiding spam complaints as well as maintaining a good sender reputation with Gmail and Yahoo:

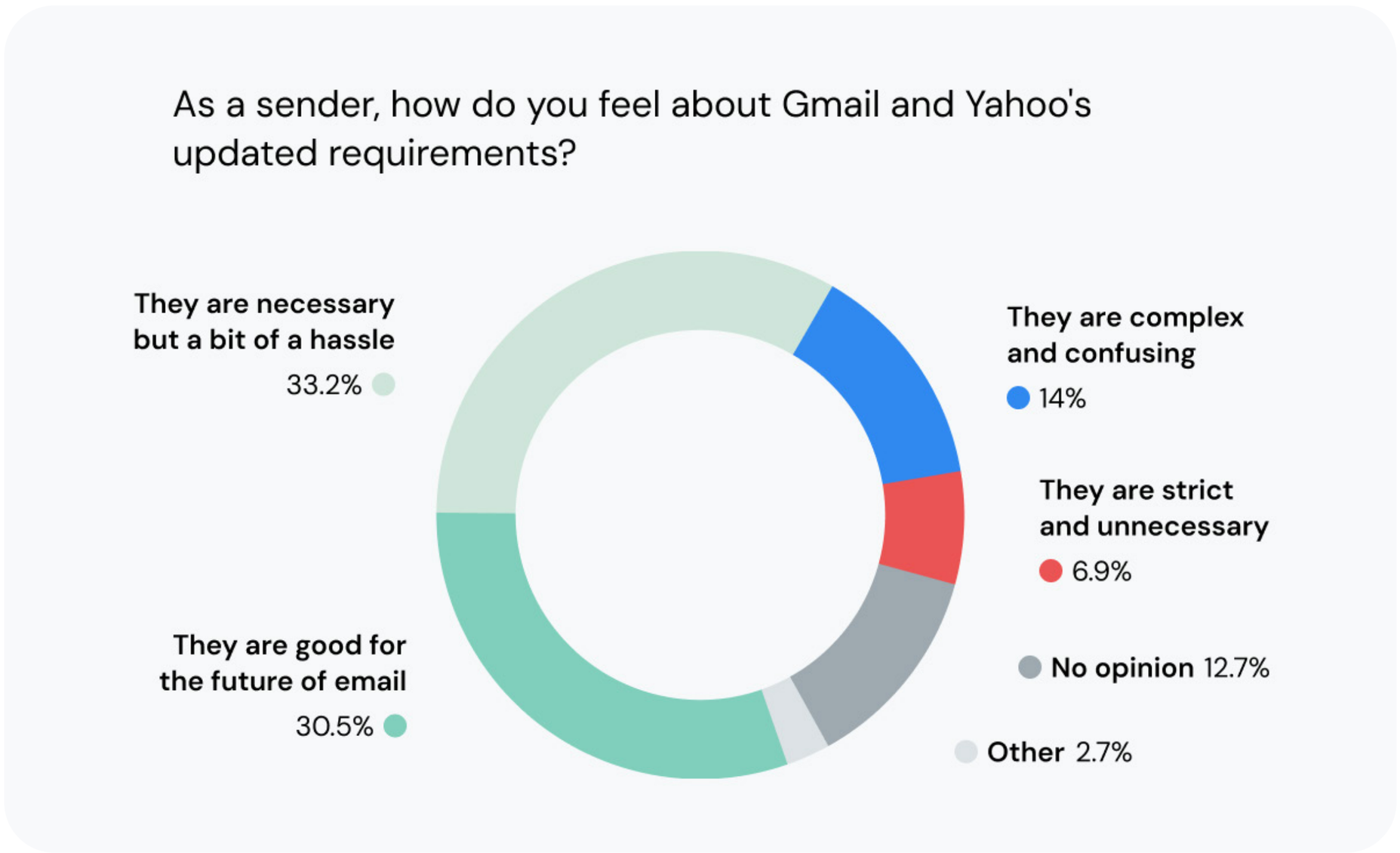
- 35.8% increased list hygiene efforts.
- 19.2% began using Google Postmaster Tools.
- 18.6% adjusted their email sending frequency.
- 12.5% changed their email opt-in process.

All the results above reflect positive changes that will not only improve the inbox experience for recipients, but they'll also support better inbox placement for the senders.

How do senders feel about the new requirements?

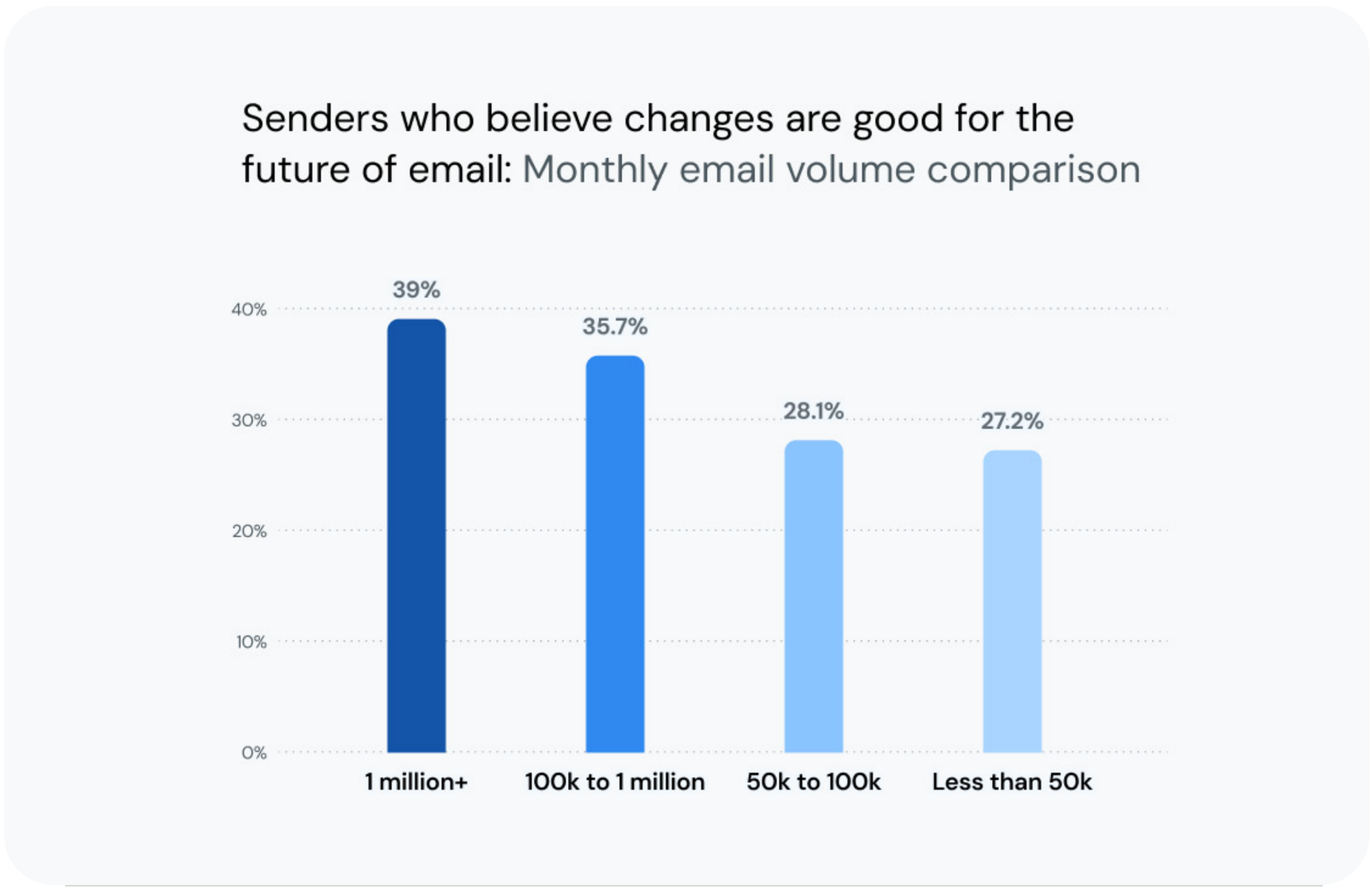
In the end, less than a quarter of the senders we surveyed (23%) reported having any deliverability challenges they attributed to Yahoo and Google's new requirements. So, Yahoogle certainly wasn't the end of the world.

Among survey respondents who told us they were familiar with the requirements, nearly 64% had a generally positive reaction: **30.5% believe the changes are good for the future of email and another 33.2% believe they are necessary** (even if they are a bit of a hassle).



Less than 7% of senders called the changes strict and unnecessary while 14% found them complex and confusing. Close to 18% had no opinion.

A higher percentage of bulk senders tend to agree with the decision to enforce these changes. **39% of respondents with the highest monthly send volumes (1 million+ per month) think the requirements are good for the future of email.** Another 38% of those senders call the changes necessary. However, those positive sentiments gradually decrease with lower volume senders who may be less equipped to address technical tasks such as email authentication.



Microsoft joins the party

When Microsoft announced new sender requirements for Outlook.com, Hotmail.com, and Live.com in early 2025, the industry reaction wasn't quite as loud as the Yahoogle shakeup of 2024. That's partly because the core rules look awfully familiar and partly because Microsoft didn't bring quite the same energy to enforcement.

Still, if you're a high-volume sender, you'll want to pay attention. Let's break down what's different about Microsoft's approach and what you actually need to do about it.

Recapping Microsoft's 2025 sender requirements

Effective May 5, 2025, Microsoft began requiring authentication from senders delivering more than 5,000 emails per day to their consumer domains. That means Outlook.com, Hotmail.com, and Live.com now join Gmail and Yahoo in enforcing baseline email security standards.

At a high level, Microsoft's sender requirements look like this:

- SPF and DKIM: Required.
- DMARC: Required, with a minimum policy of p=none, aligned with either SPF or DKIM.
- Volume threshold: More than 5,000 messages per day to Microsoft consumer inboxes.

So far, so familiar, right?

Where Microsoft diverges from Yahoogle

Unlike Gmail and Yahoo, Microsoft hasn't gone quite as hard on requirements like unsubscribes or thresholds., but here's what Microsoft **hasn't** mandated (yet): Our internal deliverability experts weighed in on why Microsoft took a different tactic

- No RFC 8058 one-click unsubscribe. Just a "visible, functional unsubscribe link."
- No required List-Unsubscribe headers.
- No explicit spam complaint threshold.
- No guidance on TLS, HELO/EHLO formatting, or forward detection.

Now, this doesn't mean that you can slide under the radar and opt out of one-click unsubscribe (unless you send zero emails to Gmail or Yahoo users). And even with the appearance of leniency, Microsoft made it clear: authentication failures or poor sender hygiene will lead to deliverability issues, whether or not there's a formal policy behind it.

The good news for senders

If you've already done the hard work to meet Gmail and Yahoo's requirements, you're set for Microsoft. That means:

- SPF and DKIM are configured and passing.
- DMARC is in place and aligned.
- You're keeping your lists clean and spam complaint rates low.
- Your unsubscribe links are visible and functional, even if not RFC 8058.

Our take: Microsoft may be riding in the backseat but still headed to the same destination

“Yahooglesoft” may sound like a clunky mashup, but it reflects a clear industry trend: inbox providers are tightening their standards, aligning on authentication, and expecting senders to keep up.

Microsoft may not be calling for one-click unsubscribes or publishing spam complaint thresholds, but the core message is clear: authenticate, clean your lists, and respect recipients.

> “The only real requirement Microsoft put in their blog post announcement was the authentication piece around requiring DMARC. But they then named recommendations which are all things that go into our reputation calculations. Merely meeting the authentication standard is not the thing that’s going to guarantee inbox placement – it’s just a bare minimum.”

Alison Gootee
Deliverability Advocacy Specialist, Sinch Mailgun

The inbox is no longer a free-for-all. And honestly? That’s good for everyone.

Making email safer and less spammy

Yahooglesoft isn’t a comic book villain squad setting out to make life miserable for senders. The goal was to make the inbox safer, more convenient, and less cluttered for their users.

Email phishing is a never-ending battle, and it’s **getting worse with AI**. Authentication protocols help thwart malicious senders by keeping them out of the inbox. So, requiring stricter authentication, including DMARC, protects both email users and senders from bad actors.

When emails are unsolicited, or even simply unwanted, they’re nothing but a nuisance. Encouraging senders to focus on delivering messages that are anticipated and relevant is a win for everyone involved. Email recipients have better experiences. Mailbox providers have satisfied users. And senders see improved email performance.

Even if you do view the stricter requirements as a bit of a hassle, the reality is they really are good for the future of email, and that’s something we should all support.

Google’s Neil Kumaran sums things up nicely...

> “These changes are like a tune-up for the email world, and by fixing a few things under the hood, we can keep email running smoothly. But just like a tune-up, this is not a one-time exercise. Keeping email more secure, user friendly and spam-free requires constant collaboration and vigilance from the entire email community.”

Neil Kumaran
Group Product Manager, Gmail Security & Trust

CHAPTER 2

Email authentication in 2025

While generative artificial intelligence (gen AI) offers plenty of promise for the future, it's also making it hard to tell what's real and what's not – especially in the wrong hands. While email senders use AI to improve efficiency and brainstorm marketing ideas, scammers and spammers found their own nefarious uses for it.

Phishing has been a major concern for years. Now, with generative AI tools, bad actors can quickly create deceptive emails to look as if they came from any brand. They can also use large language models (LLMs) to personalize scams for more convincing social engineering.

Email authentication protocols help mailbox providers identify you as a legitimate sender. It proves you are who you say you are, that your messages can be trusted, and they should be delivered to the inbox. But are enough senders using email authentication?

Key findings on Yahoo and Gmail sender requirements

63%

of senders were at least somewhat familiar with the new requirements.

49.5%

of senders who were aware of the new requirements made changes to their email programs in response.

79%

of senders who made changes updated email authentication protocols.

64%

of senders believe the new requirements are necessary or good for the future of email.

Email authentication basics

Authentication is one of the more technical aspects of email deliverability. It involves DNS records that receiving mail servers are required to reference before messages get delivered.

As a quick review, these are the DNS TXT records connected to email authentication and the basics of what they do:

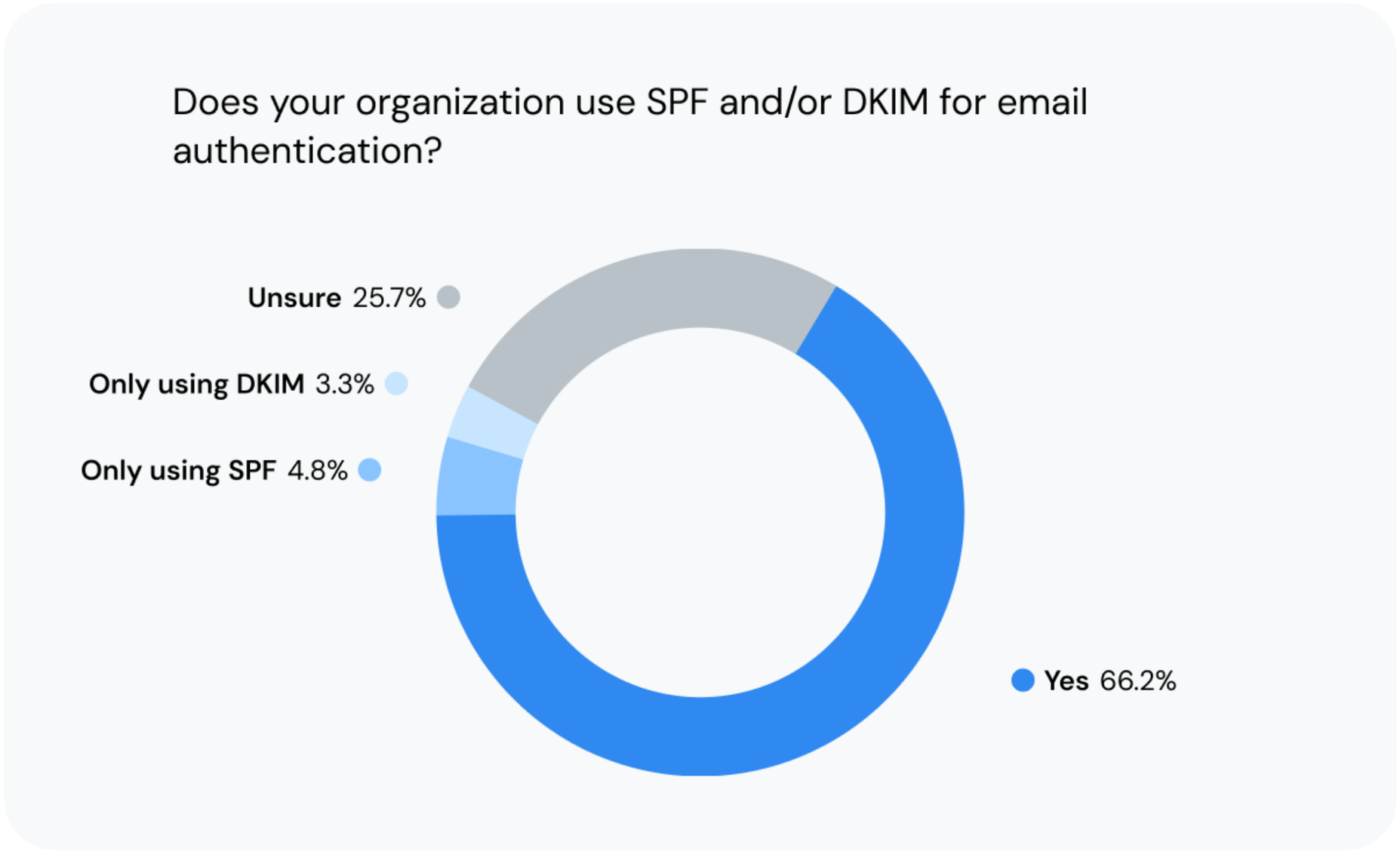
- **Sender Policy Framework:** SPF specifies which IP addresses are authorized to send emails on behalf of a domain. It helps verify that a valid source sent the email.
- **DomainKeys Identified Mail:** DKIM uses a cryptographic digital signature, which allows receiving mail servers to verify the email came from the domain it claims to be from.
- **Domain-based Message Authentication, Reporting and Conformance:** DMARC builds on SPF and DKIM by providing a way for domain owners to specify how receiving mail servers should handle authentication failures.
- **Brand Indicators for Message Identification:** BIMI builds on DMARC and allows brands to display a verified logo next to emails in the recipient's inbox when DMARC is enforced.

Bulk senders need to use SPF, DKIM, and DMARC if they want to achieve inbox placement with major mailbox providers. However, every sender can benefit from using all three of these methods – and BIMI is like the icing on the cake.

SPF and DKIM usage

The SPF and DKIM protocols are essential to email authentication. While low-volume senders may be able to reach the email inbox with just one of the two, using both is highly encouraged. **Bulk senders must use SPF and DKIM to comply with Gmail and Yahoo's 2024 requirements**.

Nearly two-thirds of all senders (66.2%) say they do use both SPF and DKIM for email authentication. 25.7% of respondents were unsure about how their organizations used DKIM and SPF. Less than 9% said they were only using one or the other.



When we filter these results based on send volumes, **more than 75% of respondents sending over 50,000 emails per month are confident they use both protocols.** The highest degree of uncertainty around SPF and DKIM came from the low-volume senders with fewer than 50,000 emails per month.

For those who are unsure about SPF and DKIM authentication, it's likely they are using at least one of them. Most email service providers (ESPs) require that these protocols are configured before any emails are sent. In some cases, an ESP may use its own SPF and DKIM records on behalf of smaller senders on shared IPs.

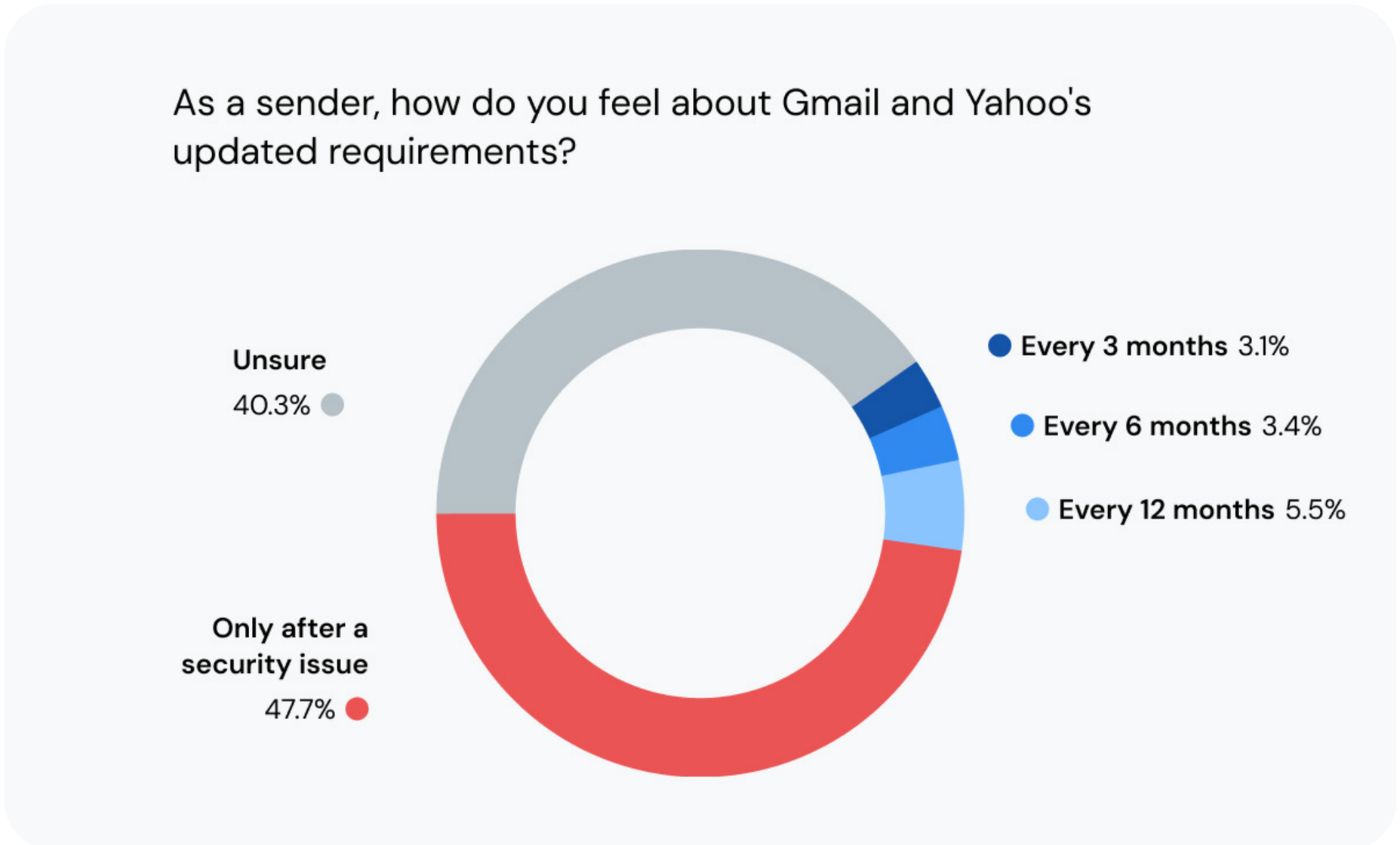
DKIM key rotation

The DKIM protocol involves a pair of keys, one public and one private, which are used to authenticate a sending domain. The private key contains the encrypted digital signature and is sent along with email messages. The public key lives on the DNS and is matched with the private key to verify the message's authenticity.

DKIM keys need to be changed periodically. This is a practice known as DKIM key rotation. It's necessary because these keys can be compromised, which opens the door for bad actors to do some real damage.

DKIM key rotation is a lot like changing your personal account passwords to keep them secure. Unfortunately, senders don't seem to be in the habit of rotating DKIM keys.

47.7% of senders who use DKIM admit they'll only rotate keys after a security issue. By then, it may be too late. Another 40% of the senders in our survey say they are unsure about DKIM key rotation practices.



Only a combined 12% of senders say they have an approximate timeframe for rotating DKIM keys. The other 88% could be putting their customers and subscribers as well as their brand's reputation at risk.

If someone steals your DKIM keys, they don't even need to use spoofing. They are literally able to sign emails as if they were sent from your domain.

It's considered best practice to rotate DKIM keys every 6 to 12 months at minimum. If your DKIM keys are leaked or a bad actor manages to decipher them, change keys as soon as possible. Visit the Sinch Mailgun help center to learn how to **update or rotate your DKIM keys**.

EMAIL SECURITY FEATURE

Get automatic DKIM key rotation

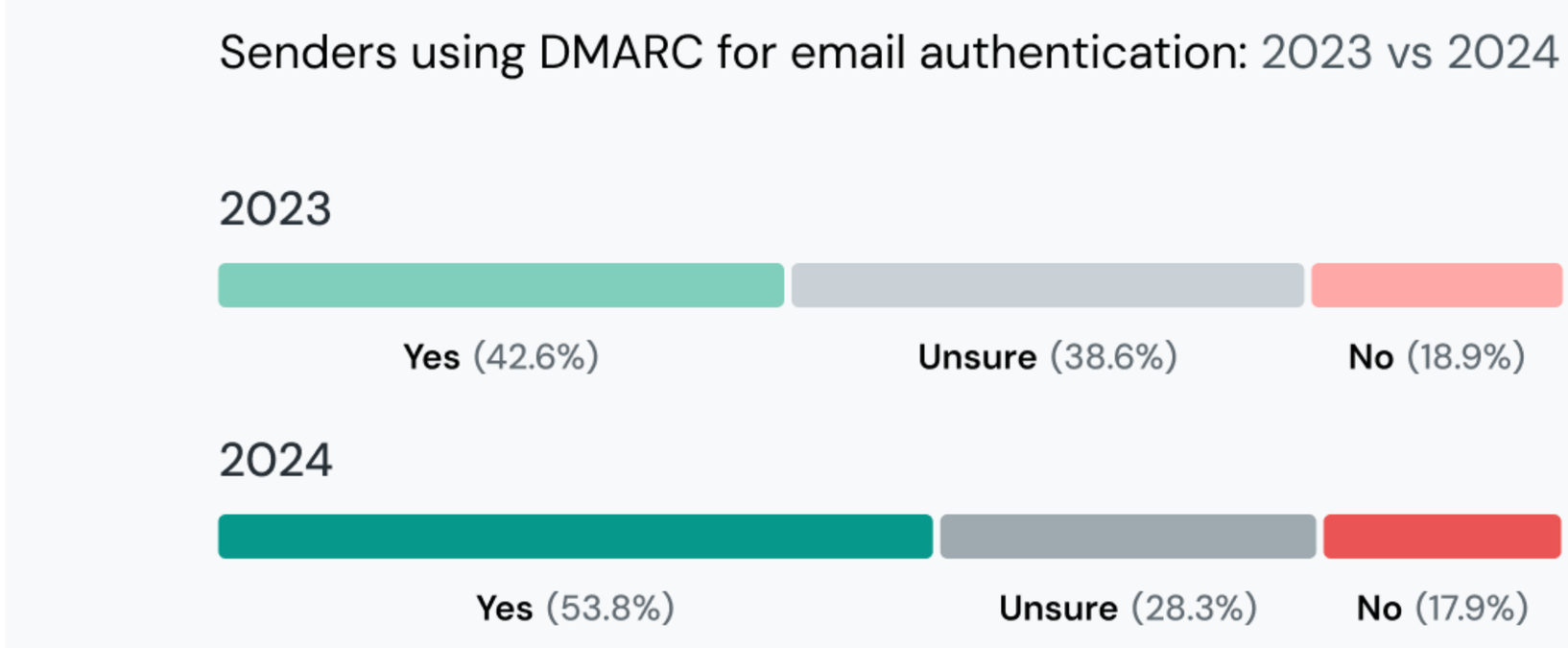
Here's one less thing to worry about. Sinch Mailgun users enjoy extra security and peace of mind with a new feature that automates DKIM key rotation. If you use Mailgun Send, you can choose to have 2048-bit DKIM keys updated every 120 days. Manually rotate your keys whenever it's needed.

Find out more

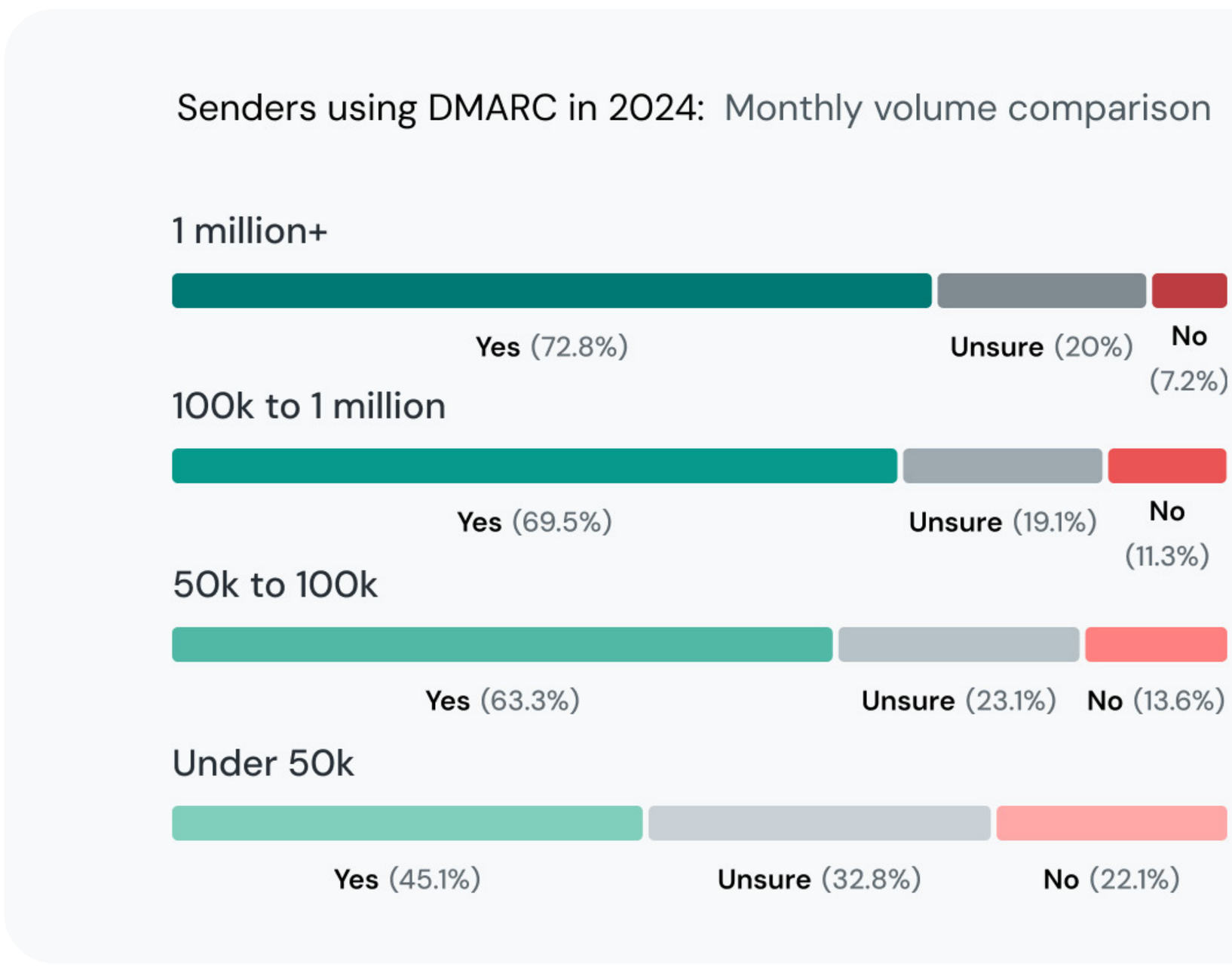
DMARC adoption

It's fair to say the most important aspect of Google and Yahoo's new rules for bulk senders is the DMARC requirement. DMARC offers a way to harness the power of both SPF and DKIM for strong email authentication.

Our survey results show an uptick in DMARC adoption compared to the results we published in **State of email deliverability 2023**. **In 2024, 53.8% of senders told us they were using DMARC.** That represents an 11% increase from the 42.6% who'd implemented DMARC in 2023.



As you might expect, due to the Google DMARC requirement, the increase appears even stronger among bulk senders. While around 56% of the highest volume senders had set up DMARC in 2023, approximately 70% or more of them had done so in 2024.



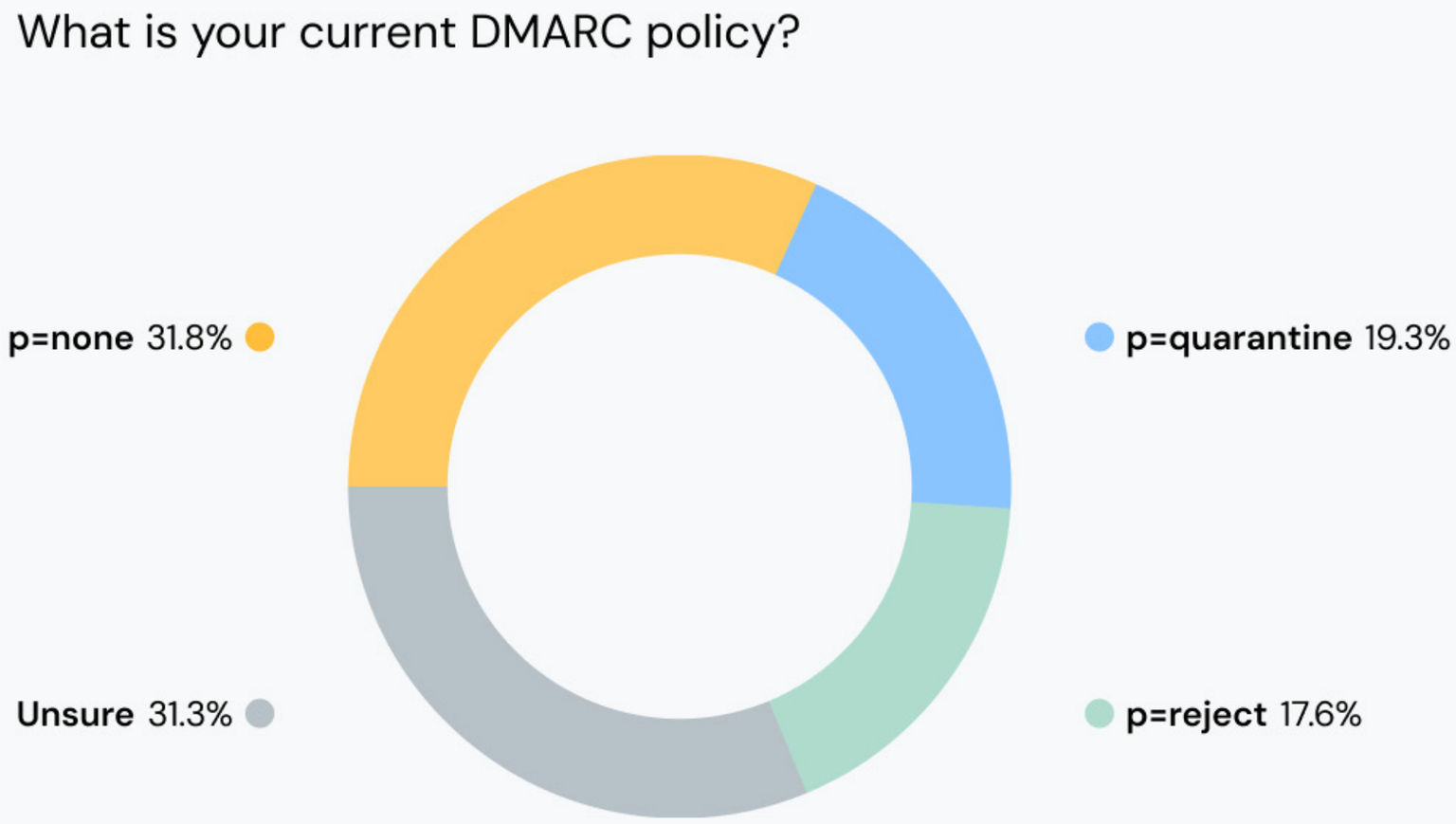
DMARC policies

When setting up DMARC, senders must choose a specific policy that informs receiving mail servers how to handle messages that fail SPF or DKIM. Here's how each of the three policies work:

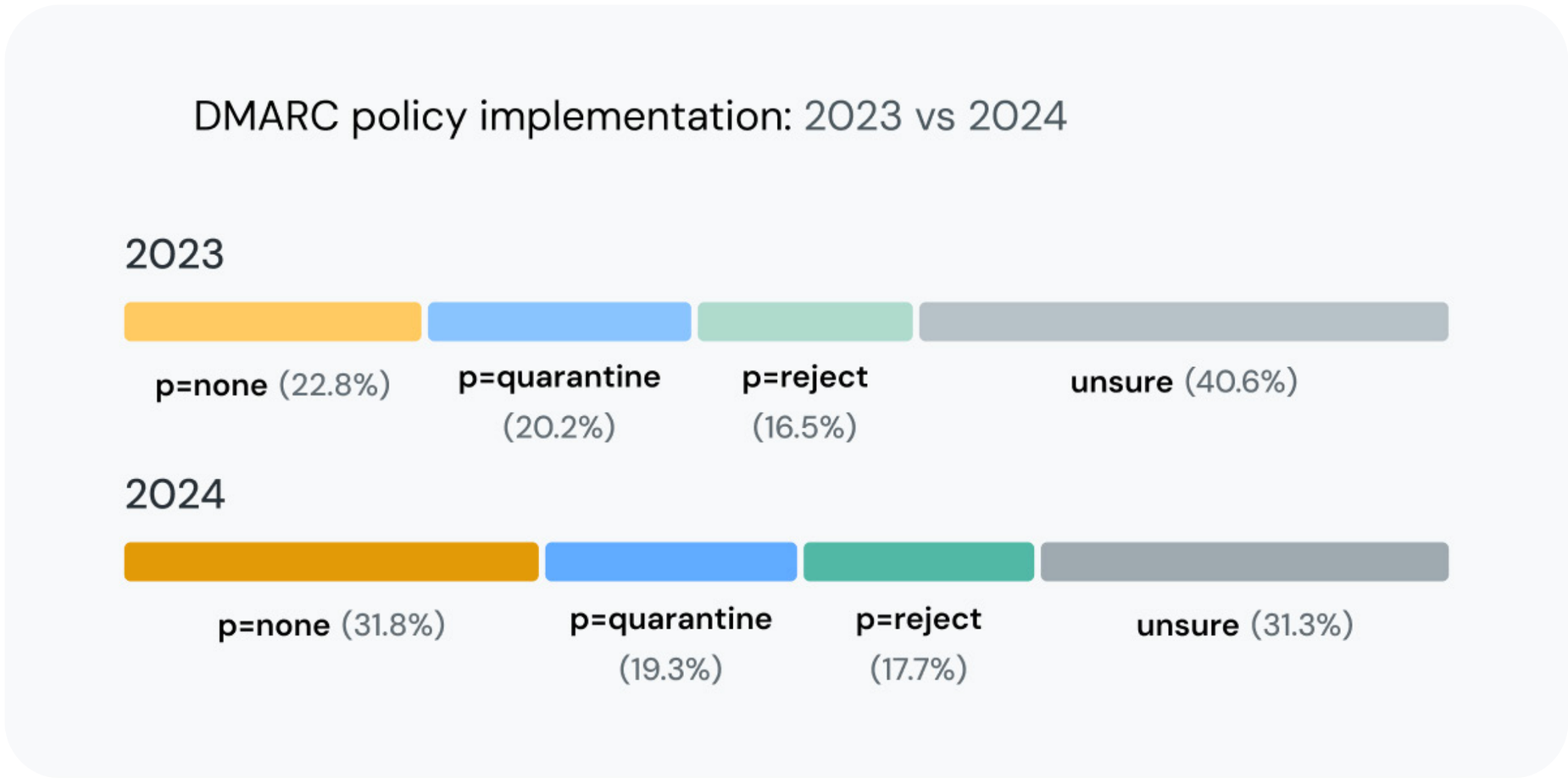
1. **None** (p=none): This DMARC policy tells receiving mails servers not to do anything if a message fails authentication.
2. **Quarantine** (p=quarantine): This DMARC policy tells receiving mails servers that authentication failures should be filtered into spam.
3. **Reject** (p=reject): This DMARC policy is the strongest. It tells receiving mails servers that authentication failures should not be delivered at all.

The Yahoo and Google DMARC requirement only dictated that senders use a policy of p=none. That's because, at this point, the mailbox providers are trying to get senders to take the first step towards enforcement.

The p=none policy was the most common policy senders used in 2023, and it remained that way in our latest survey. **31.8% of senders who use DMARC have their policy set to None, 19.3% are using Quarantine, and 17.7% have a policy set to Reject.**



In 2023, around 23% of senders had DMARC policies set to None. But the most noticeable change was a decrease in senders who are uncertain about what policy is used. While 31.3% of senders in this year's survey are unsure of their DMARC policy, that dropped from more than 40% in 2023.



This result suggests the new sender requirements not only encouraged DMARC adoption, but it also increased awareness around the standard and its specific policies.

DMARC requirements today and tomorrow

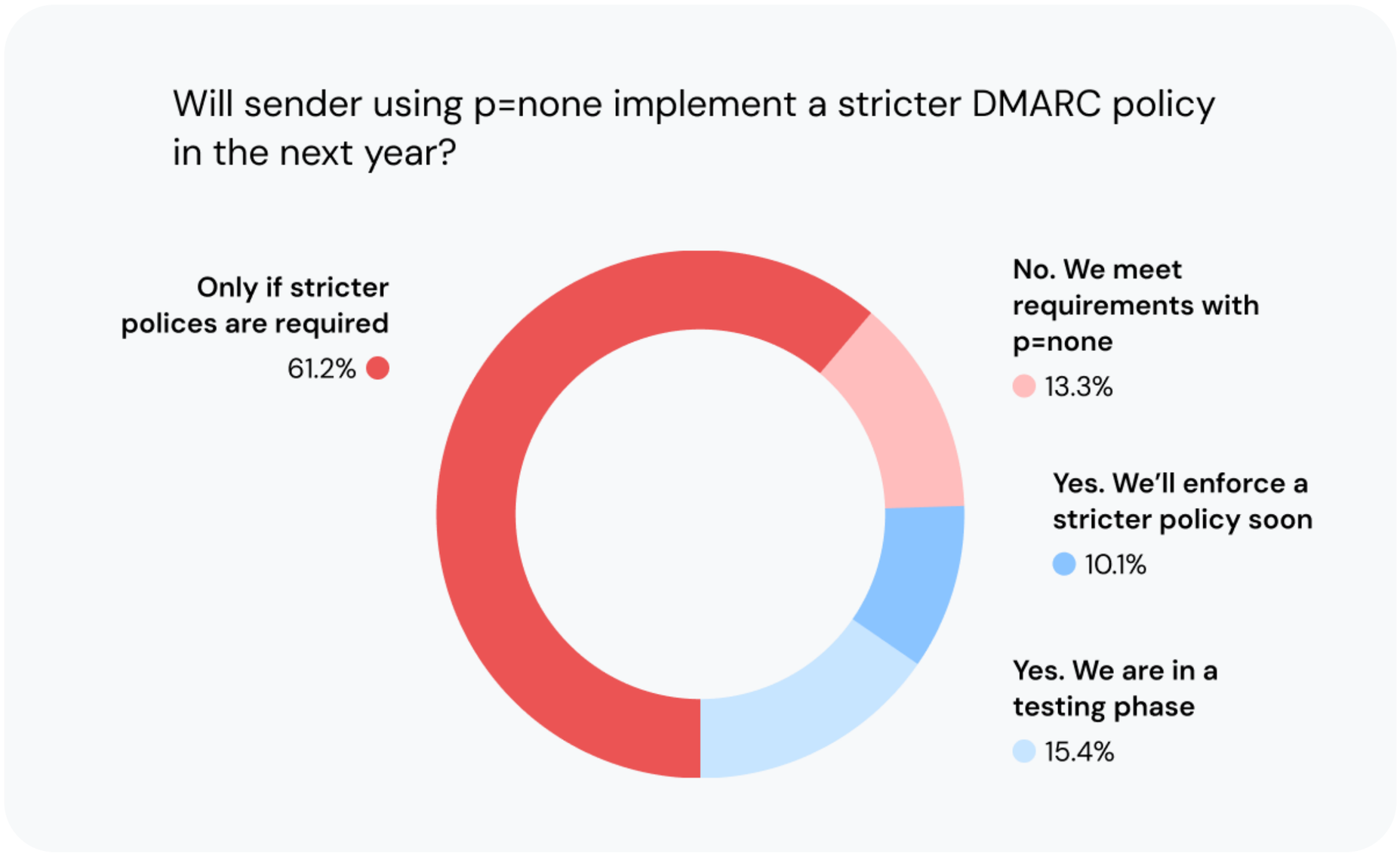
There's a problem with using the p=none DMARC policy. It doesn't exactly do much to improve your authentication. Messages that fail DKIM or SPF may still be delivered to email inboxes. **Technically, you aren't enforcing DMARC until you implement a policy of p=quarantine or p=reject.**

> "DMARC actually fills in a gap that SPF and DKIM both kind of left behind, introducing the concept of alignment... it closes that loophole and makes sure that you are who you say you are. You get to set a DMARC policy that says: reject, quarantine, or monitor. Right now mailbox providers aren't requiring anything stricter than p=none, but that could change." - Alison Gootee Deliverability Advocacy Specialist Sinch Mailgun"

Alison Gootee
Deliverability Advocacy Specialist, Sinch Mailgun

The p=none policy is meant to be used to test DMARC during setup. Eventually, senders are supposed to change the policy. So, is that what senders in our survey plan to do?

Results show a combined 25.5% of senders using p=none plan to update the policy within the next year. However, **61% will only do so if they are required** and 13% don't plan to update because they meet the current DMARC requirements.



Senders who plan to wait until DMARC enforcement is required may not be waiting long. Representatives from Gmail and Yahoo told us they'll eventually call for a stronger policy. Senders who've taken steps to enforce DMARC are ahead of the game – and they're doing the right thing.

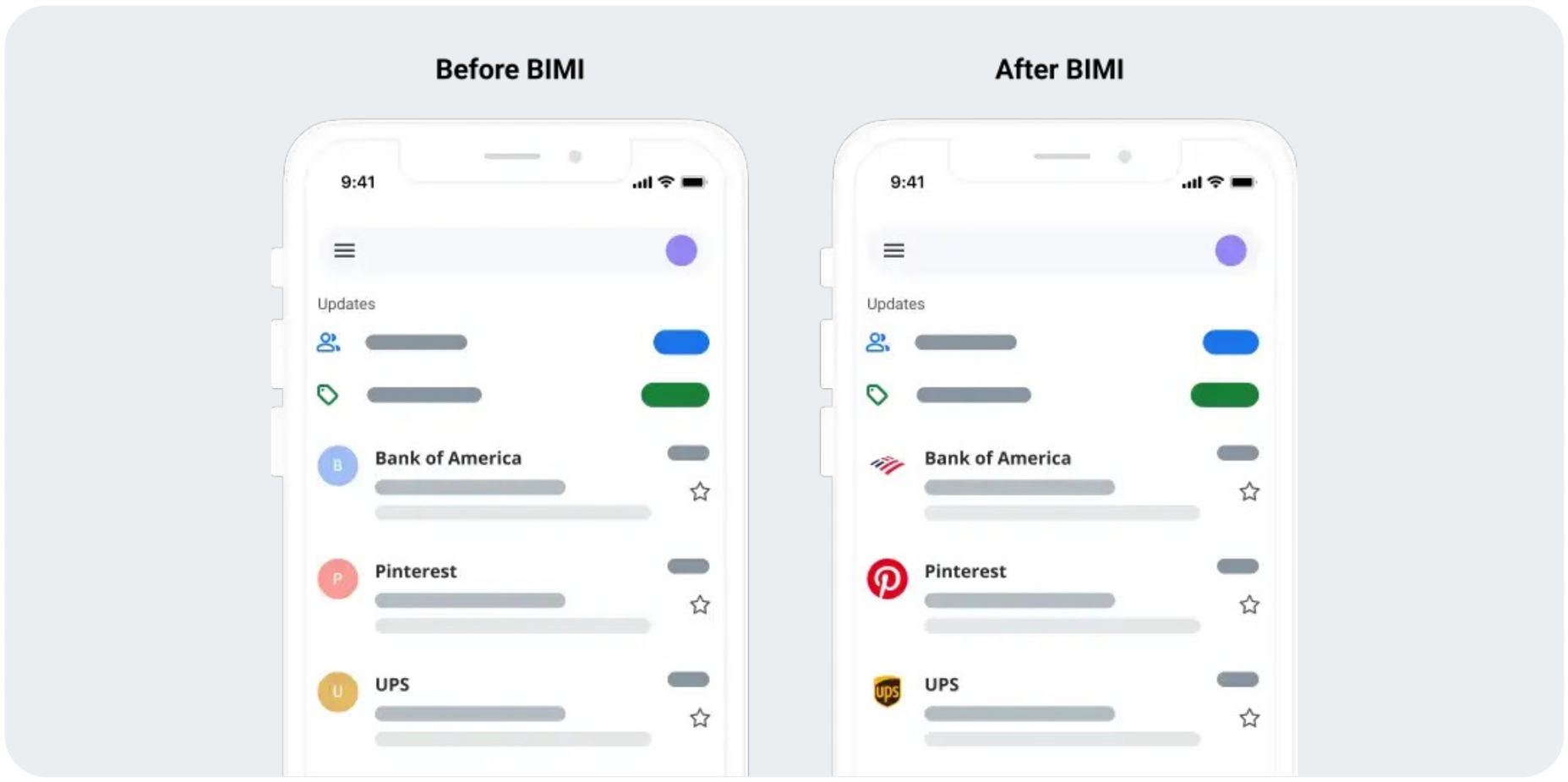
> "The end goal is ideally a policy of p=reject. That's what DMARC is for. Ensuring that your domain cannot be spoofed and protecting our mutual customers from abuse."

Marcel Becker
Senior Director of Product at Yahoo

BIMI implementation

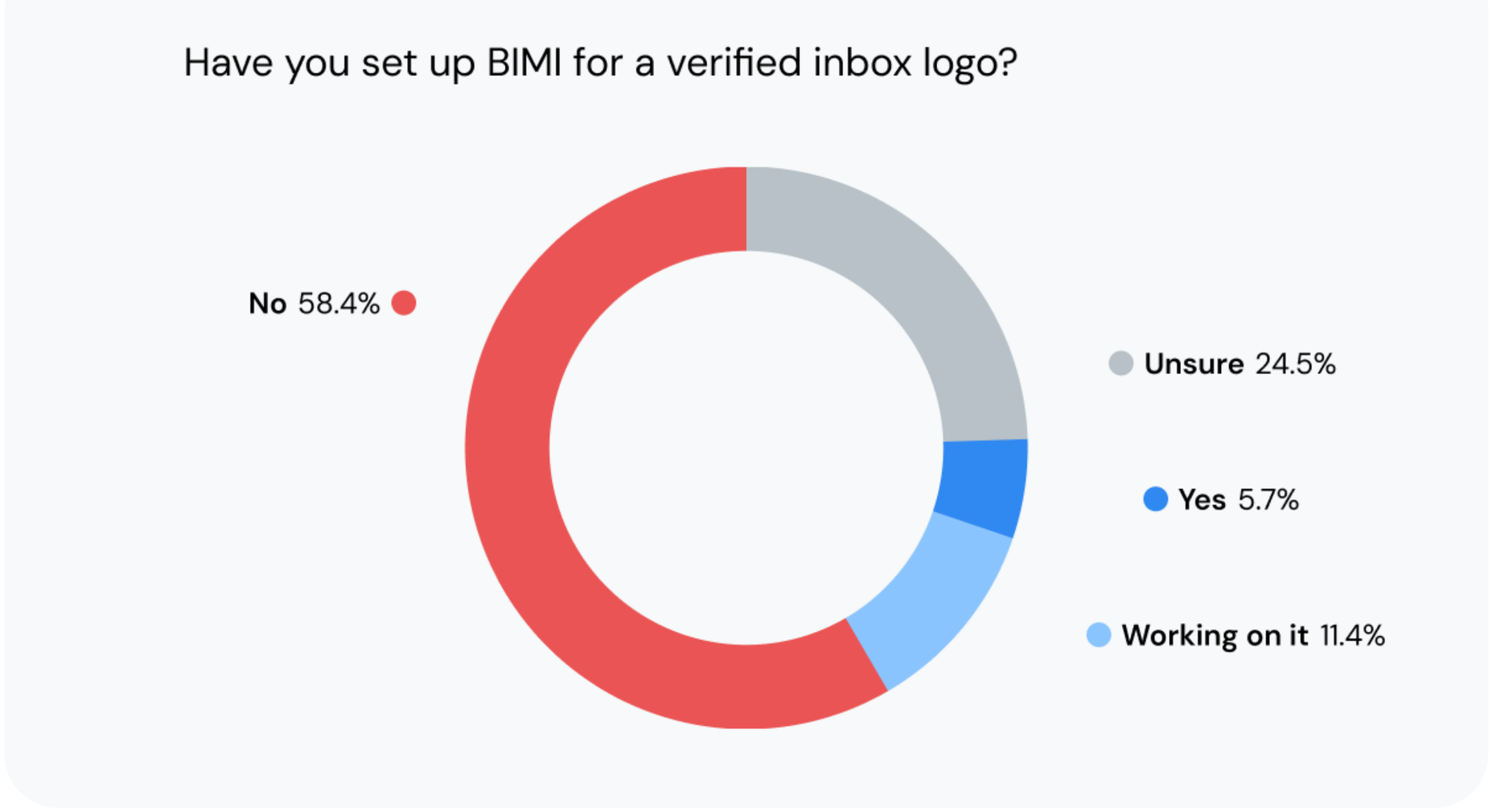
If you need another reason to choose a stronger DMARC policy, maybe BIMI will do the trick. This specification lets senders display a verified logo next to their emails. To be eligible for a BIMI logo, however, **you need to be enforcing DMARC with a policy of Reject or Quarantine.**

Gmail, Apple Mail, and Yahoo Maill all support BIMI, but Outlook currently does not. Here's how a BIMI logo might look in the inbox:



So, how popular is BIMI? The website BIMI Radar tracks more than 72-million domains for what it calls "BIMI-readiness." As of this writing, the site indicates only 3.8% of those domains would be eligible for a BIMI logo. That means the vast majority aren't using DMARC or don't have a strong enough policy.

Our latest survey asked email senders if they'd already implemented BIMI. Results show 5.7% of respondents use BIMI while another 11.4% are working to implement the specification. Still, nearly 60% of senders are not using BIMI.



BIMI does not directly impact deliverability or do anything to authenticate your emails. Nonetheless, it gets associated with authentication because only senders who've put in the effort around DMARC can display a verified inbox logo. As you can imagine, this has advantages for many brands.

Why do senders pursue a BIMI logo?

We wanted to find out what prompted the senders who are using BIMI to pursue an inbox logo. What did they expect to gain from it? Here's what those senders say was the **primary driver of BIMI implementation:**

30.3%

Customer/subscriber trust

22.3%

Protecting brand reputation

21.8%

Building brand awareness

13.3%

Email security

An inbox logo certainly provides some extra branding via your emails. While BIMI itself does not do anything to enhance email security, it's proof that a sender has taken other steps to do so. Recipients may be more likely to open and engage with emails displaying an inbox logo because it appears more trustworthy.

7.4% of respondents told us they pursued BIMI to boost email engagement. And that could very well be true. A **2021 study on inbox logos** suggests they positively impact engagement metrics such as open rates.

Why email authentication is worth the effort

Setting up email authentication can get complex, but all the work pays off. It's a win for everyone involved… except spammers and scammers

Why email authentication is worth the effort

How email authentication benefits senders:

- Keeps your brand from being spoofed.
- Protects customers from security threats.
- Supports a good sender reputation.
- Leads to better inbox placement.

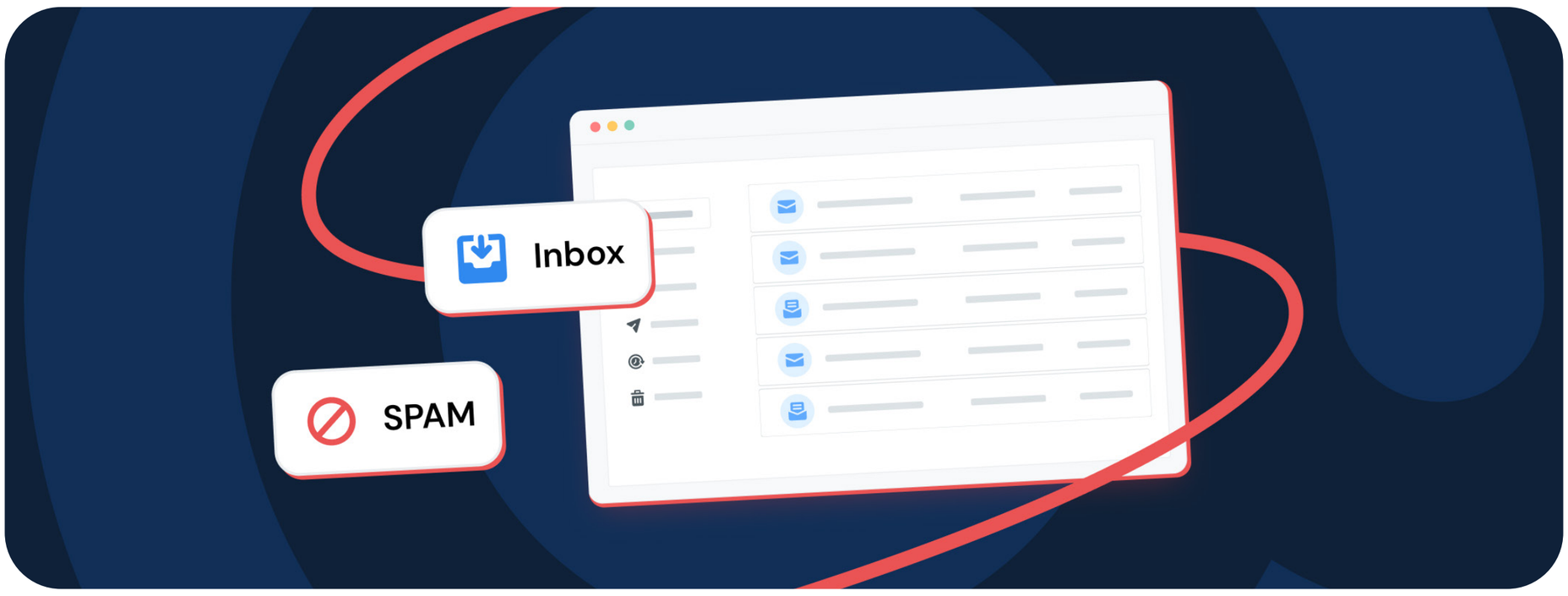
How email authentication helps mailbox providers:

- Helps identify legitimate senders vs malicious messages.
- Supports the integrity of their product.
- Keeps people using email for brand communications.
- Offers guidance on filtering authentication failures.

How email authentication supports recipients:

- Stops phishing emails, spam, and malware from reaching their inboxes.
- Creates trust for brands they want to hear from.
- Improves the inbox experience by reducing unwanted emails.

Our survey results show the email community is making progress with authentication and inbox security, but there's still room for improvement.



CHAPTER 3

Understanding inbox placement

For as technical as email deliverability gets, the goal is straightforward. **You don’t want emails blocked, you want to avoid spam folders, and you need to reach the inbox.** Of course, that may be easier said than done, especially if you have no idea what happens to your messages after they’re sent.

What if we told you, you’ve been measuring inbox placement all wrong? In this chapter, we’re going to expose one of the biggest misconceptions in email deliverability.

Measuring deliverability and inbox placement

A variety of metrics provide insights into email deliverability, but which one are you using to find out if emails make it to the inbox?

When we asked 1,100 senders to select the metrics and methods they actively use to measure email deliverability, these were the top five responses:

1. Open and click rates (57.4%)
2. Delivery rate (53.1%)
3. Bounce rates (46.5%)
4. Unsubscribe rate (39.5%)
5. Spam complaints (32%)

Email engagement metrics, such as opens and clicks, are important to monitor. You want to maintain good email engagement to achieve inbox placement. When your contacts open and click, it's a sign to mailbox providers that your emails are wanted. A sudden drop in typical open and click rates may also indicate there are deliverability problems.

Conversely, a high unsubscribe rate can signal that your emails are unwanted. While it's normal to have contacts unsubscribe, if the rate increases, you may have an issue with the sending frequency or relevancy of your emails.

Getting marked as spam is one of the fastest ways to end up in the spam folder, so it's surprising that **less than one-third (32%) of senders say they are actively monitoring the spam complaint rate.** This seems to be an undervalued metric, especially considering the sender requirement of a 0.3% threshold for spam complaints.

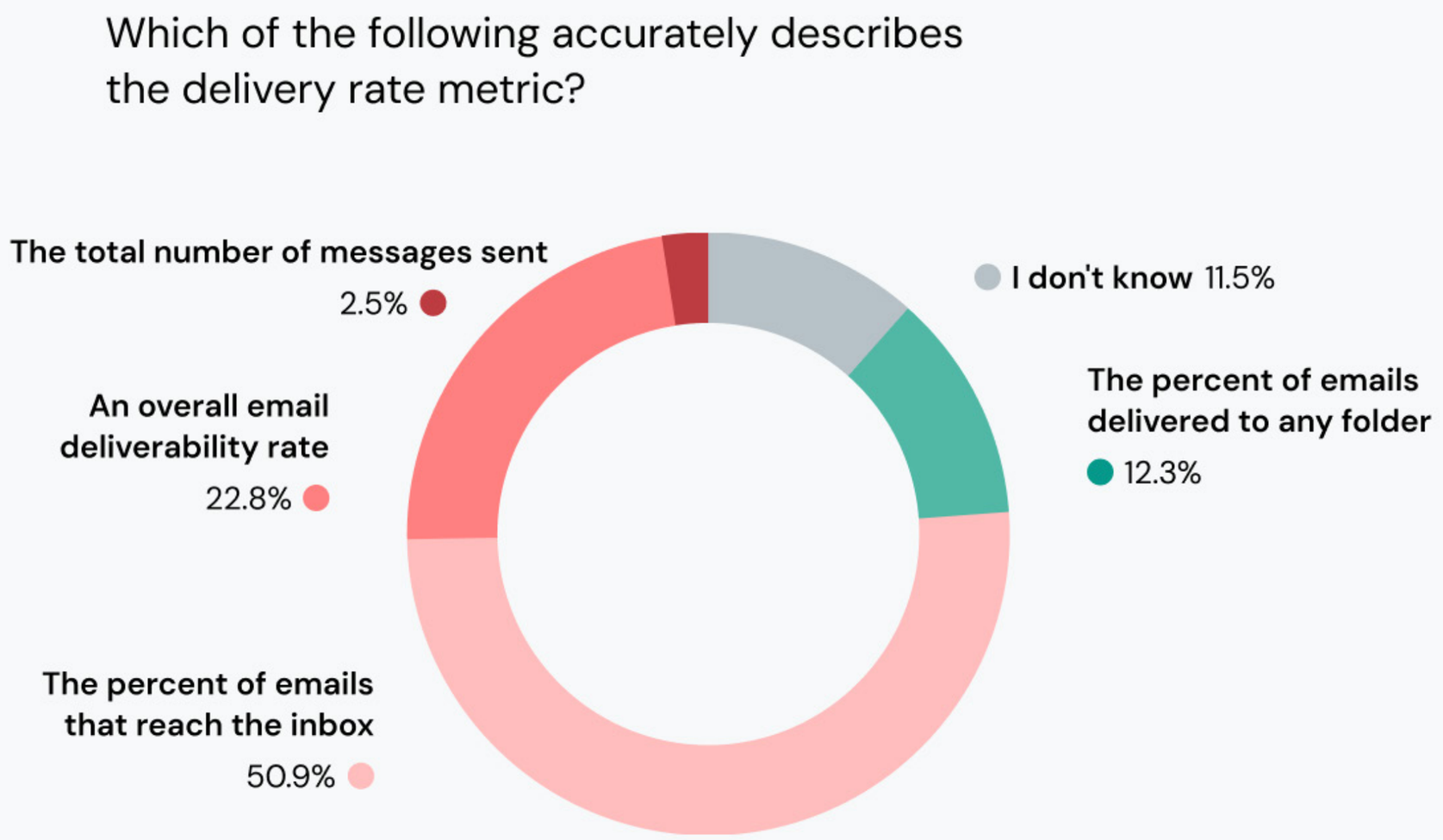
53% of senders actively monitor their delivery rate. That's the second most-common metric among all respondents. However, the delivery rate does not measure what most senders think it does.

The truth about your email delivery rate

In somewhat of a twist, we threw a “quiz question” into the State of email deliverability 2025. We wanted to know how senders define the email delivery rate. What do they think it measures? 11.6% could admit they didn’t know. The rest were willing to make a guess:

- ✗ 50.9% think the delivery rate is the percentage of emails that reach the inbox.
- ✗ 22.8% think the delivery rate measures overall email deliverability.
- ✗ 2.5% think the delivery rate measures the total number of emails sent.
- ✓ 12.3% know the delivery rate is the percentage of emails delivered to any folder.

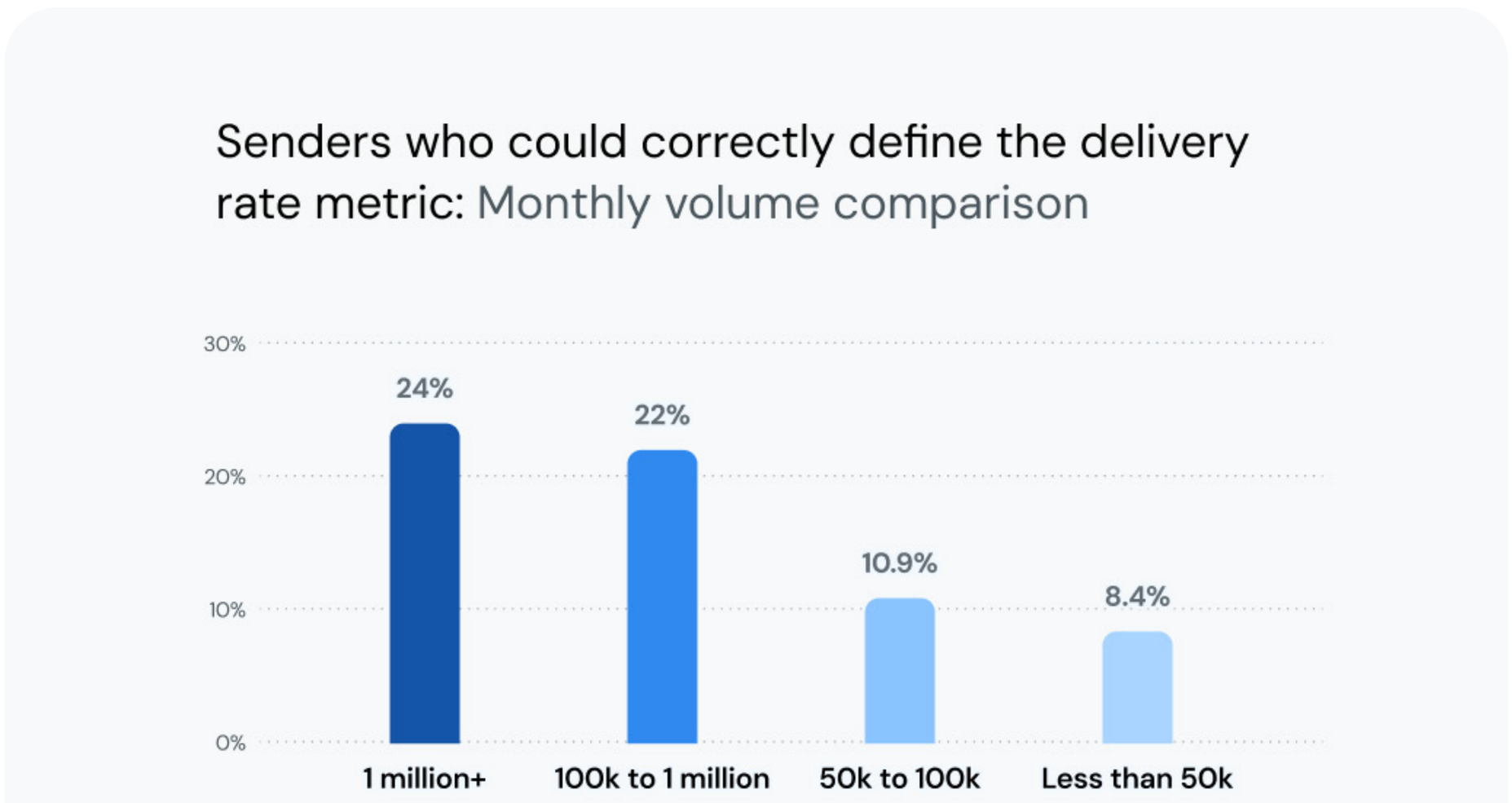
Shockingly, this means **almost 88% of senders in our survey could not correctly identify what the delivery rate measures.** This is perhaps the biggest misconception in email deliverability. It’s time to clear things up



The delivery rate metric measures the percentage of emails accepted by a receiving mail server and delivered to any folder. **When emails land in spam, it still counts towards the delivery rate.** Those emails were delivered… to the junk folder. The only messages that don’t count toward the delivery rate are those that bounce or get rejected by the receiving mail server.

So, if you have a delivery rate of 98%, you know that most of your emails were delivered. But what you don’t know is if you were able to avoid spam.

Senders with larger email volumes were more likely to answer the delivery rate question correctly. Nevertheless, more than 3/4 of those senders still got it wrong. Less than a quarter of the highest volume senders (24%) could correctly define the delivery rate



This may leave you wondering how you can measure where your emails land. Is there a way to know if you'll reach the inbox or get filtered into spam? **There is... it's called the inbox placement rate** and the only way to uncover it is with a specific type of **email testing.** Unlike the delivery rate, inbox placement testing tells you what happens to emails that get delivered.

Here's how the inbox placement rate is calculated:

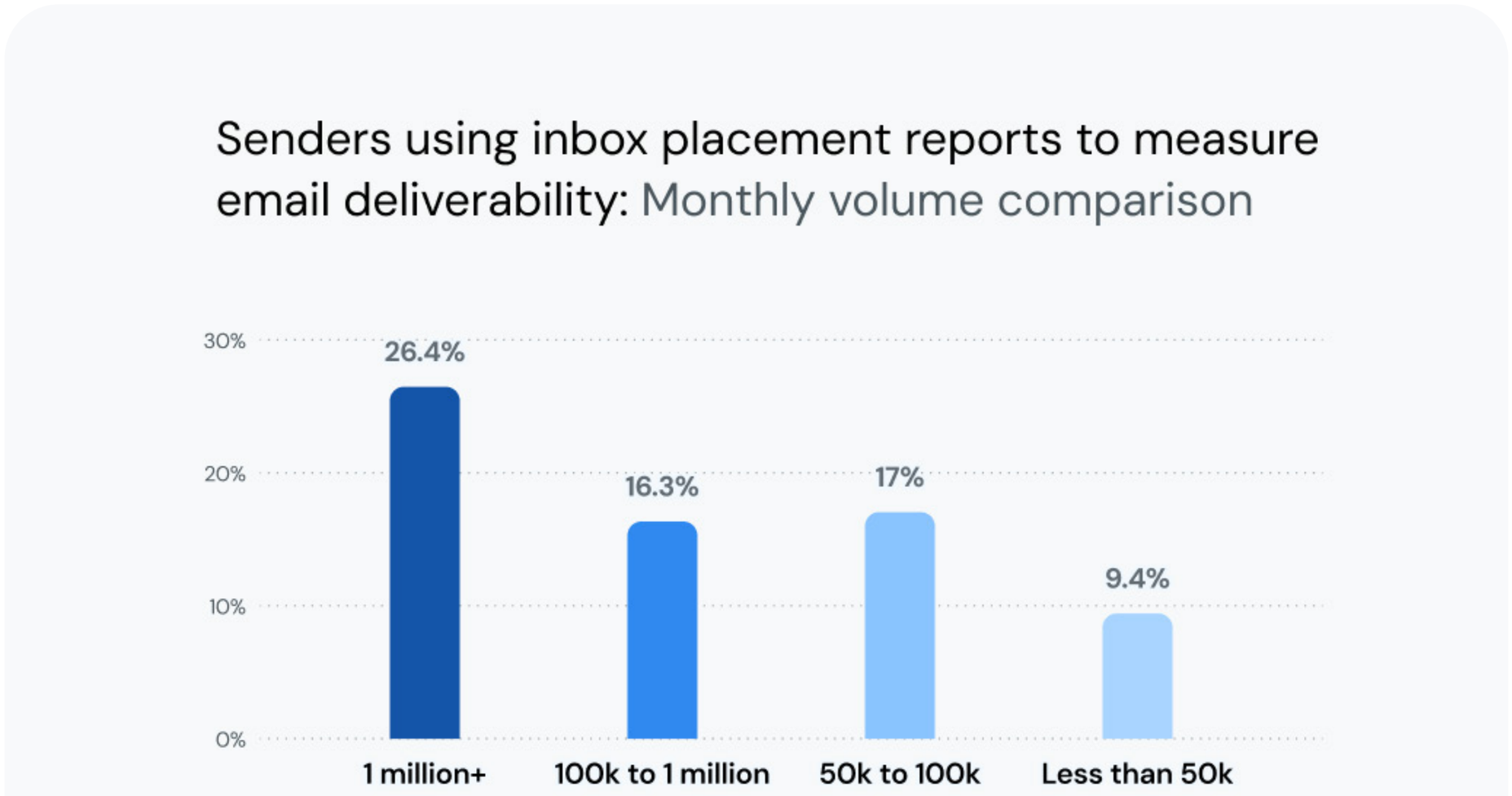
```
Inbox placement rate % = (# of messages in the inbox ÷ # of messages delivered) X 100
```

> The delivery rate measures the percentage of emails that receiving mail servers accept, which includes emails that end up in spam folders.

How inbox placement testing works

The inbox placement rate isn't a metric that shows up in your typical email analytics. That's probably why so few senders in our survey are using it.

Only 13.3% of respondents use inbox placement reports to measure email deliverability. That percentage does increase based on email send volumes. But even among organizations sending more than one million emails per month, only about 1 in 4 conduct inbox placement testing.



Inbox placement testing is also known as “seed testing.” That’s because the process uses seed mailboxes from major providers to find out where your messages end up. In the end, you get a report providing visibility into inbox placement.

Here’s how inbox placement testing works:

Step 1 - Send a test email to a list of seed mailboxes:
Your or a partner owns this list, and it will include major providers (Gmail, Yahoo, Outlook, etc.) Receiving mail servers filter the test email based on numerous factors.

Step 2 - Monitor email delivery:
Track where the test email ends up in each seed mailbox. Inbox? Spam/junk? Promotions tab? Blocked?

Step 3 - Analyze results and adjust:
Review the results of your inbox placement report. If there are issues, identify what you may need to change to improve deliverability.

If necessary, you can retest your email after adjusting. Results from inbox placement reports can reveal issues like blocklisting and authentication failures. They’ll also help you optimize future sends for improved deliverability.

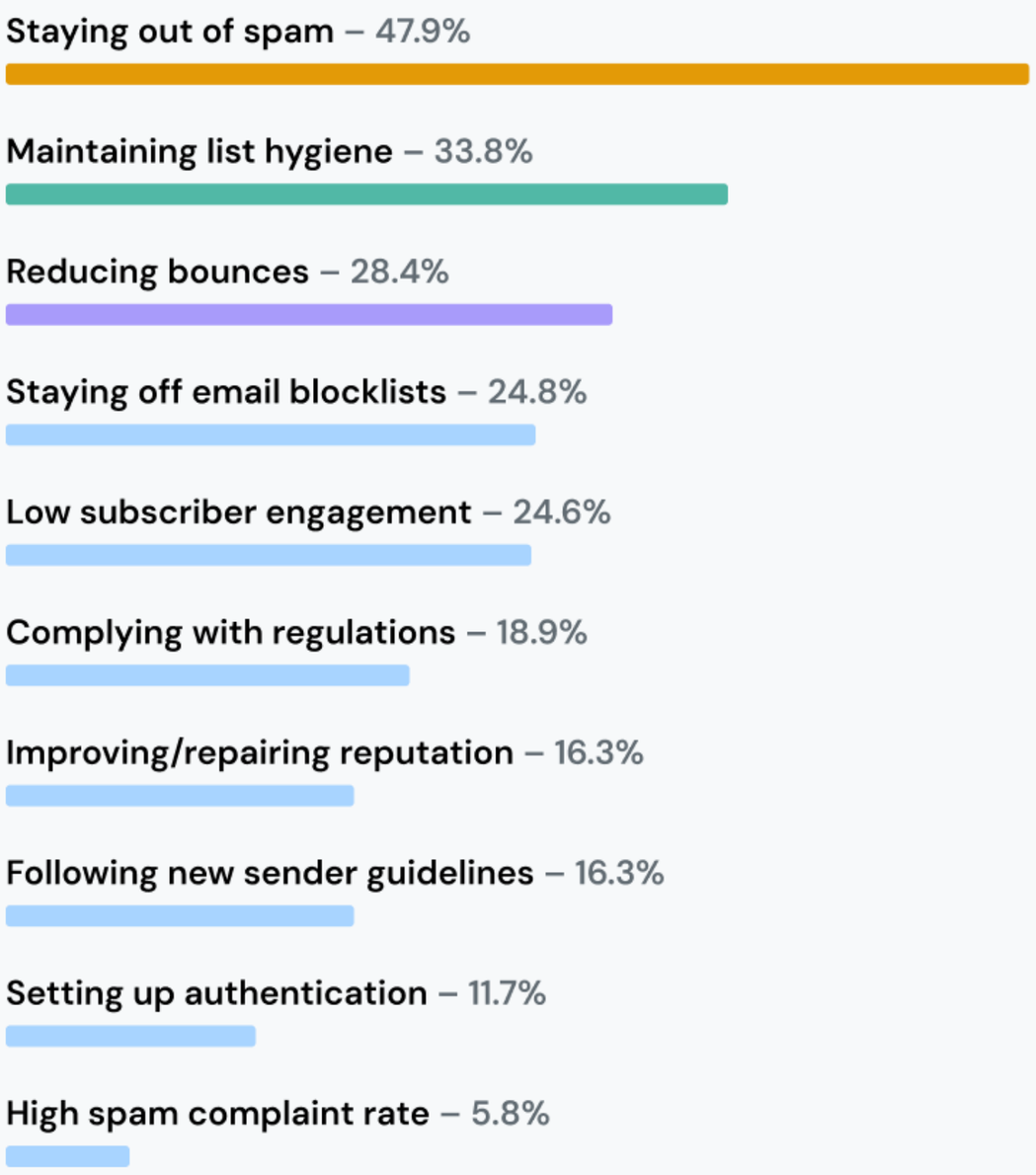
Deliverability challenges: Quick tips to avoid spam

Inbox placement testing is the best way to help you take on the main challenge in email deliverability – avoiding the spam folder.

When we asked senders to select their top three email deliverability issues, staying out of spam emerged as the clear winner. **48% of all senders cited staying out of spam as a top challenge.** That's followed by maintaining list hygiene at nearly 34% and reducing bounce rates at around 28%.

What are your biggest email deliverability challenges?

Respondents selected up to three



Higher volume senders were less likely to cite avoiding spam as a challenge and more likely to have challenges with low subscriber engagement and list hygiene than smaller senders.

Your customers aren't too happy when emails land in spam either. That's especially true if it's a message they're anticipating. When we surveyed consumers for the Sinch Mailgun report, **Email and the customer experience**, we found **many people have a negative reaction when a brand's emails land in spam.**

35.4%
don't worry about it.

32.8%
feel annoyed/frustrated.

10%
lose trust in the brand.

9.9%
unsubscribe.

While some consumers won't care or don't notice if your emails land in spam, that's not necessarily a good thing. It suggests they're so uninterested in what you're sending that it doesn't matter where your messages end up.

How to stay out of spam

Here's some essential advice to prevent your emails from going to your contacts' spam folders. These are basic tips, but they'll go a long way towards improving inbox placement.

1. **Set up email authentication:** This verifies your **identity as the sender** and supports your reputation with mailbox providers.
2. **Obtain consent first:** Before you add a contact to your email marketing list, be sure to get permission. A **double opt-in process** helps confirm intent to subscribe.
3. **Make it easy to unsubscribe:** When contacts can't opt out, they mark you as spam instead. Follow **RFC 8058 for one-click unsubscribe** and honor requests as soon as possible.
4. **Monitor user complaints:** Keep a close eye on your **spam complaint rate**. Strive to keep it under 0.1% and only send emails your contacts want to receive.
5. **Comply with regulations:** Make sure you follow key laws including the EU's GDPR, the CAN-SPAM Act, and other **data privacy regulations**.
6. **Keep your list clean:** Manage your contacts by keeping invalid email addresses and **spam traps** off your lists. Segment or remove unengaged subscribers.
7. **Conduct inbox placement testing:** Know if you're likely to be filtered into spam before you send by **reviewing inbox placement reports** from seed mailboxes.

To sum it all up – if you want to avoid the spam folder, don't act like a spammer.

Email blocklist monitoring

What's worse than being filtered into spam? Ending up on an **email blocklist**. Blocklists are directories of IP addresses and/or domains that get flagged as sources of suspicious behavior, malicious content, or spam.

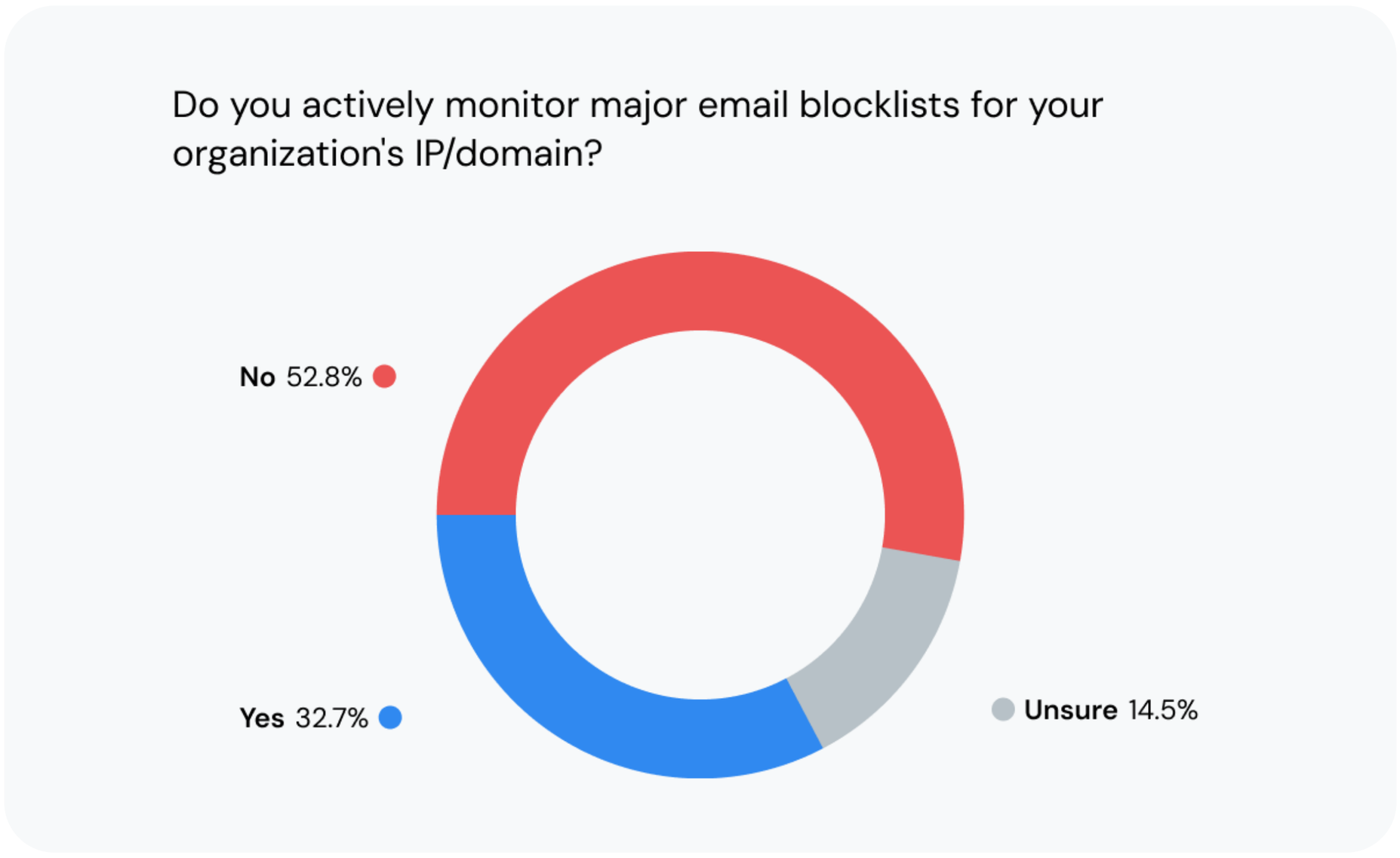
There are many reasons why you could be placed on a blocklist, sometimes it's your fault and sometimes it's not. Either way, it's a situation you'll want to remedy quickly. Here are some common explanations for being blocklisted:

- You've been emailing people without their consent.
- You're on a shared IP along with senders who have a bad reputation.
- You ramped up sending volume without **warming a new domain or IP address**.
- Your spam complaint rate got too high.
- You sent an email to a spam trap after buying a list of contacts.
- You violated consumer privacy laws.
- You lack proper email authentication.

While blocklist providers such as Spamhaus and Barracuda are willing to work with reputable senders, they aren't in the habit of alerting anyone about landing on their lists. Why would they want to tip off real spammers and scammers?

Blocklist monitoring is an email deliverability practice that alerts senders if their domain or sending IP ends up on one of the "naughty lists." Monitoring blocklists allows you to address the problem before it negatively impacts your business.

Our survey found **32.7% of senders are monitoring blocklists but more than half are not and 14.5% are unsure.**



A **blocklist monitoring service** could save your organization from some serious headaches. Imagine what would happen if transactional emails such as order confirmations and password resets were blocked by a major mailbox provider. What if a Black Friday email campaign was blocked from reaching consumers?

> “Landing on a blocklist can impact your bottom line as well as your future sending. By proactively monitoring and addressing blocklist issues as they arise, you can safeguard your reputation, maintain customer trust, and ensure your messages aren’t automatically flagged as spam.”
>
> 
>
> **Kate Nowrouzi**
> VP of Deliverability and Product Strategy at Sinch

Email bounce rates and what they mean

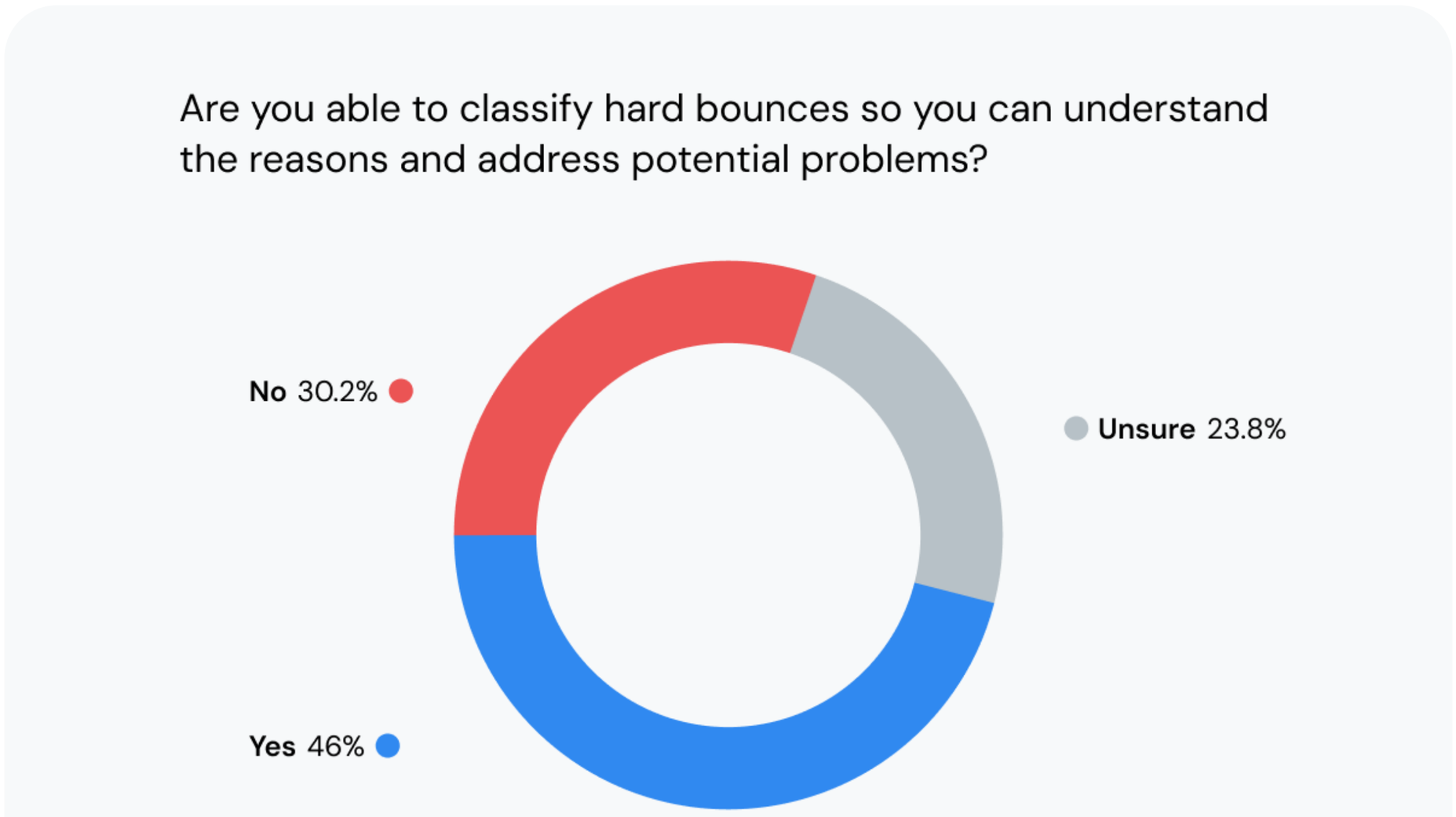
Another reason emails fail to reach the inbox is because they’ve bounced. There are two main types of email bounces:

1. **Hard bounces represent permanent delivery failures.** They’re typically caused by an invalid recipient address or non-existent mailbox. Mailgun will automatically add contacts to your suppressions list when you receive a hard bounce.
2. **Soft bounces represent temporary delivery failures.** Reasons they occur can include a server outage, full mailbox, oversize files/messages, a blocklisting, or reputation issues.

> Sinch Mailgun treats soft bounces as permanent failures, meaning we will not automatically attempt to redeliver the message. The recipient address will not be added to the suppression list, and the next time you attempt to send a message to this recipient we will attempt to deliver.

So, hard bounces are more serious. They suggest you need to remove invalid emails from your list, fix authentication protocols, or mitigate a blocklisting issue. But how do you know what's really going on?

We asked senders how well they understand hard bounces. Almost 24% of respondents said they were unsure about classifying hard bounces, 20% said they couldn't classify them and 46% said they could.



We're a little skeptical that 46% of senders truly understand how to classify hard bounces. While many email service providers (ESPs) show you hard and soft bounce rates, you might have to dig deeper to see the full picture.

When a message bounces, the receiving mail servers returns a specific **email bounce code**. These bounce classification codes represent different reason emails weren't delivered.

Here are some examples of bounce codes:

- **5.1.1** indicates a hard bounce because of bad destination mailbox address such as an invalid email.
- **5.2.2** indicates a recipient's mailbox exceeded its storage limit.
- **4.4.7** indicates a message took too long to be delivered and expired.

There are many others, including email bounce codes for SPF, DKIM, or DMARC failures. A hard bounce could also indicate a reputation issue with a provider like Gmail. Being able to classify hard bounces means you get specifics on what needs to be fixed. That's why **Sinch Mailgun offers bounce classification**. It helps users focus on the critical bounces that need attention.

More than a quarter of senders say reducing and addressing bounces is a top email deliverability challenge. Understanding email bounces is vital to both maintaining a high delivery rate as well as list hygiene. The more you know, the easier it is to address high bounce rates

.

CHAPTER 4

Email list building and hygiene

Your email list is an invaluable asset. It's how your organization connects with people through a top communication channel. Many businesses would grind to a halt without email, and around **75% consumers prefer email** for business communication.

Important assets like your contact database need to be protected and treated with care. That includes how you build your email list as well as how you manage and maintain it. As your list grows, so does your business. And as a business grows so does its email database.

In this chapter, we'll find out if senders realize just how important list building and hygiene are to email deliverability.

How does your email list impact deliverability?

Why would mailbox providers care about the database you use to send email messages? What does your list of contacts have to do with achieving inbox placement? Here's the answer... **The quality of your list and the way your contacts engage with your emails send signals about what kind of sender you are.**

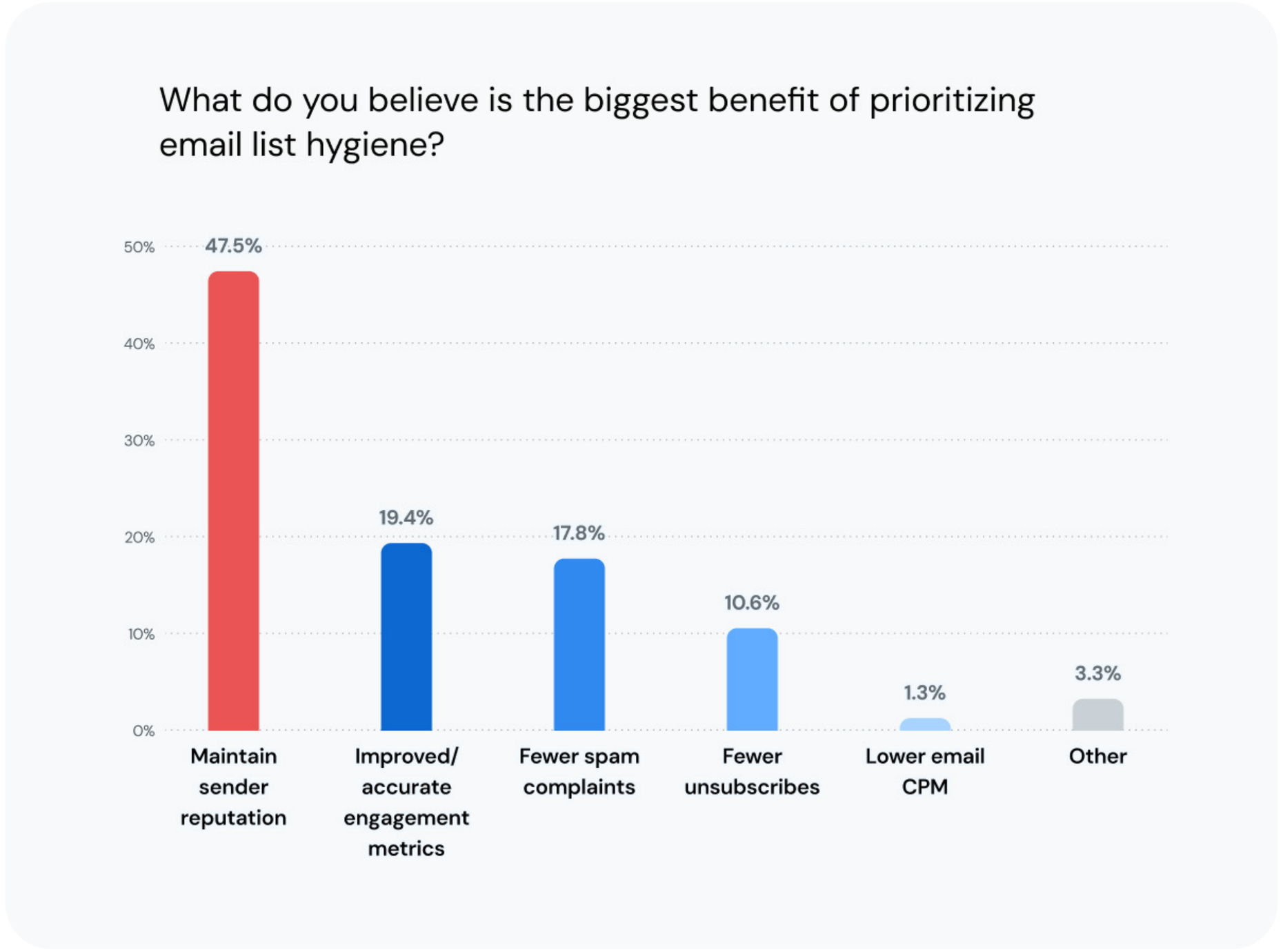
Imagine a parent checking out a teenager's bedroom. If it's a mess of fast-food wrappers, dirty laundry, and unfinished homework, that parent might assume the teenager is lazy and irresponsible. Maybe that teenager doesn't deserve certain privileges.

Likewise, to earn the privilege of reaching inboxes, you've got to keep your act clean. Here's what that means for email list building best practices:

1. Get explicit consent from contacts before adding them to your marketing list.
2. Keep subscribers engaged and spam complaints low to show your emails are wanted.
3. Use email validation to avoid addresses with typos, outdated contacts, and spam traps.
4. Regularly conduct email list hygiene to strategically segment, reactivate, or remove unengaged subscribers.

When you focus on these things, mailbox providers are much more likely to see you as a reputable sender who deserves inbox placement. The senders who took our survey find that to be true.

Among those who prioritize list hygiene, 47.5% say the biggest benefit is maintaining a good sender reputation with mailbox providers like Gmail, Yahoo Mail, and Outlook. Better engagement metrics (19.4%) and fewer spam complaints (17.8%) also emerged as top benefits, and that's also correct.



We take a closer look at sender reputation in Chapter 5 of this report. If you're unfamiliar, this is a unique score mailbox providers give senders based on a variety of factors. The health of your email list contributes to several of those factors.

> “We often compare email sender reputation to credit scores. In both cases, one costly mistake can easily damage your credit score or your sender reputation, but they take time to build back up. That’s why you need to take steps to maintain a good reputation with mailbox providers.”

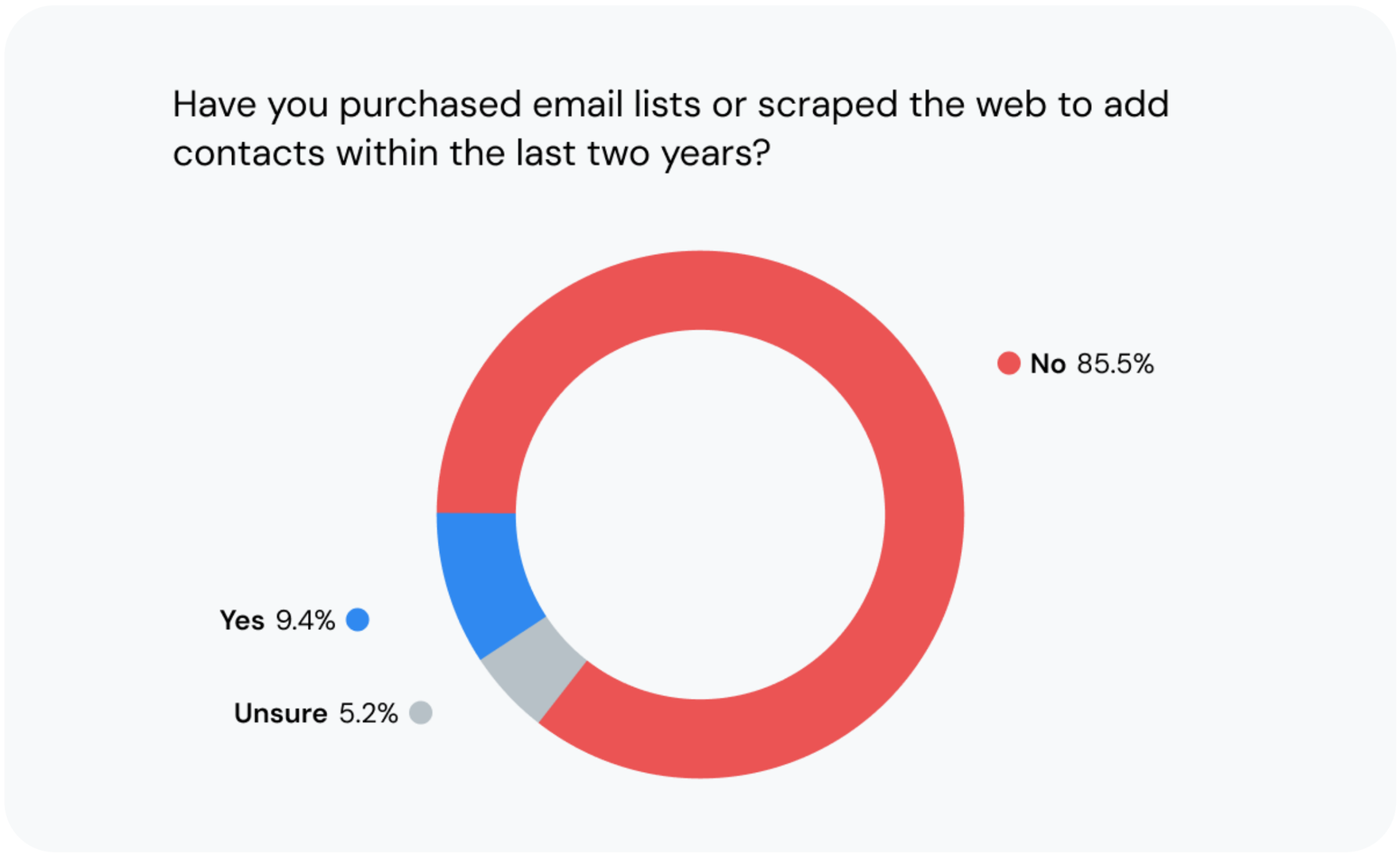
Ashley Rodriguez
Deliverability Engineer II at Sinch Mailgun

Email list building practices

The foundation of a healthy contact list starts with how you collect email addresses and confirm someone’s intent to subscribe. Obtaining proper consent, especially for promotional messages, is critical to any email program.

If you’re emailing people without consent, you are a spammer, and your messages belong in the junk folder. What’s more, without **explicit consent**, you may be violating important consumer privacy laws and could face significant fines.

Unfortunately, questionable methods are still being used. **Nearly 1 out of 10 senders in our survey (9.4%) admit they’ve either purchased email lists or scraped the web for contacts in the last two years.**



The good news is that 85.5% of the senders in our survey have not used these practices in the last couple of years while about 5% are unsure. But just wait… there’s more bad news.

When we look at monthly send volumes, it turns out that organizations sending more email are also more likely to add contacts to their lists without obtaining consent. Around 15% of senders with volumes between 100,000 to more than 1 million emails per month admit to these questionable practices.

Sinch Mailgun research also found that **B2B senders are almost three times as likely to use questionable list building methods** compared to B2C (12.3% vs 4.3%). Purchasing lists and scraping are tactics often used for cold emailing B2B prospects from the sales team. It's one thing to cold email people individually, but once it's automated for scale, you're entering the world of spammers.

Building a qualified email list organically takes time and effort. You've got to overcome the temptation to simply buy a list of contacts that fits your target audience or there could be consequences.

Nearly 1 in 10 senders admit to using questionable list building practices in the last two years. These methods will hurt deliverability and make list cleaning an urgent priority.

A better way to build your email list

There are many ways to collect contacts without spamming people and violating privacy laws:

- Place signup forms on key pages of your website.
- Start an industry newsletter to attract relevant subscribers.
- Offer valuable content in exchange for contact information.
- Allow people to subscribe to regular deals or product updates.
- Collect emails during online checkout or at the point of purchase.

However, even after someone fills out a form, there's another step you can take that supports email deliverability. It's called a **double opt-in,** and it involves sending an initial email to new contacts asking them to confirm their intent to subscribe.

In case you didn't know, here's how a double opt-in process typically works:

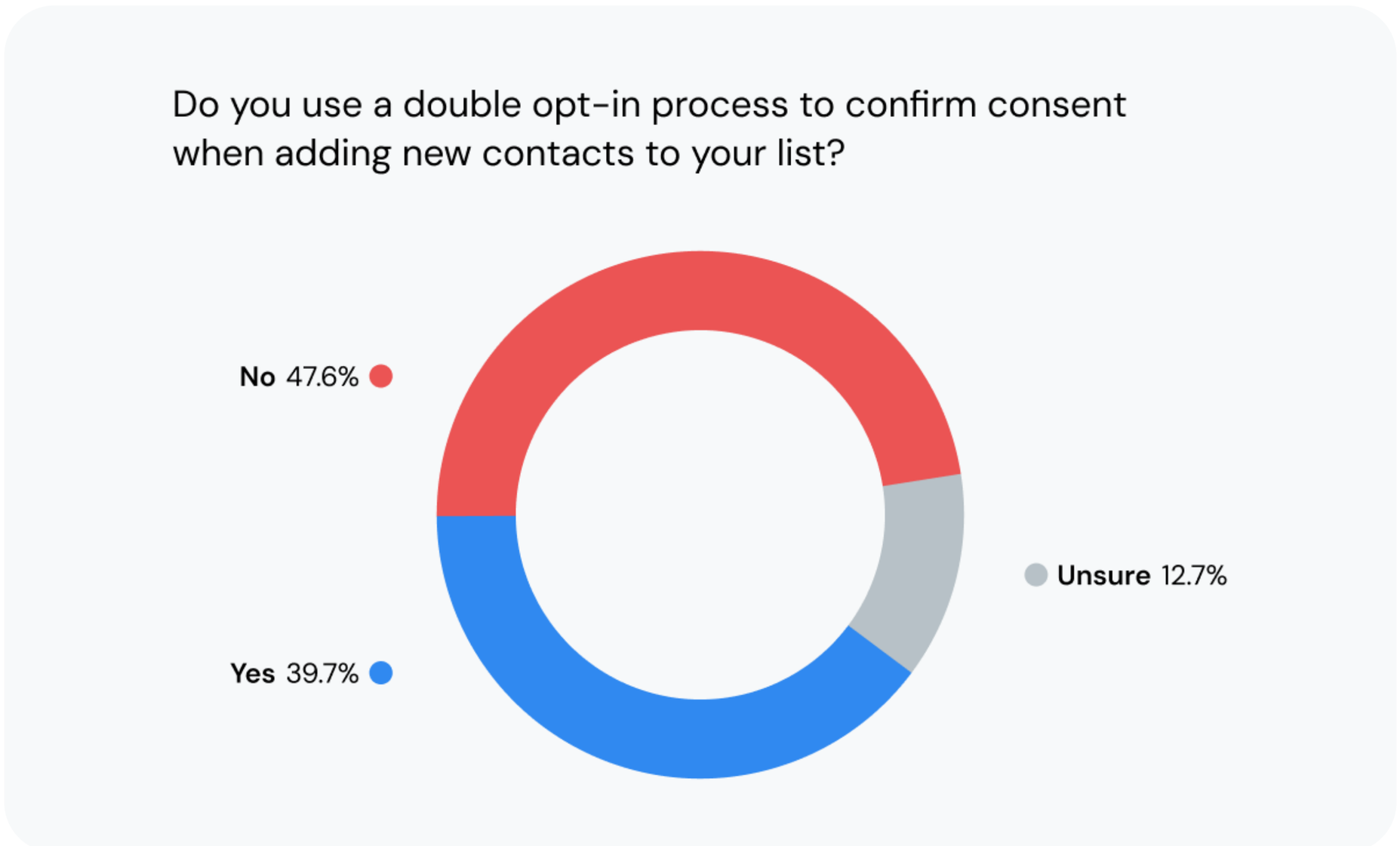
1. A new contact fills out a signup form.
2. They receive an email asking them to click a link to confirm.
3. If they click the link to confirm, you add them to your list.
4. If there's no confirmation, you don't add them or segment them into a separate list.

This process does mean list growth may be a bit slower. However, it also ensures you're only adding new contacts who really want to be on your list. These contacts are more likely to engage with what you're sending.

"I would recommend that every sender use a double opt-in all the time. Not only does it ensure you only acquire subscribers who are more likely to engage, but it also helps prevents bots from abusing signup forms, which is a significant email security risk."

Nick Schafer
Sr. Manager of Deliverability & Compliance, Sinch Mailgun

Sinch Mailgun's research shows **nearly 40% of senders are using the double opt-in method** while more than 47% are not and about 13% are unsure.



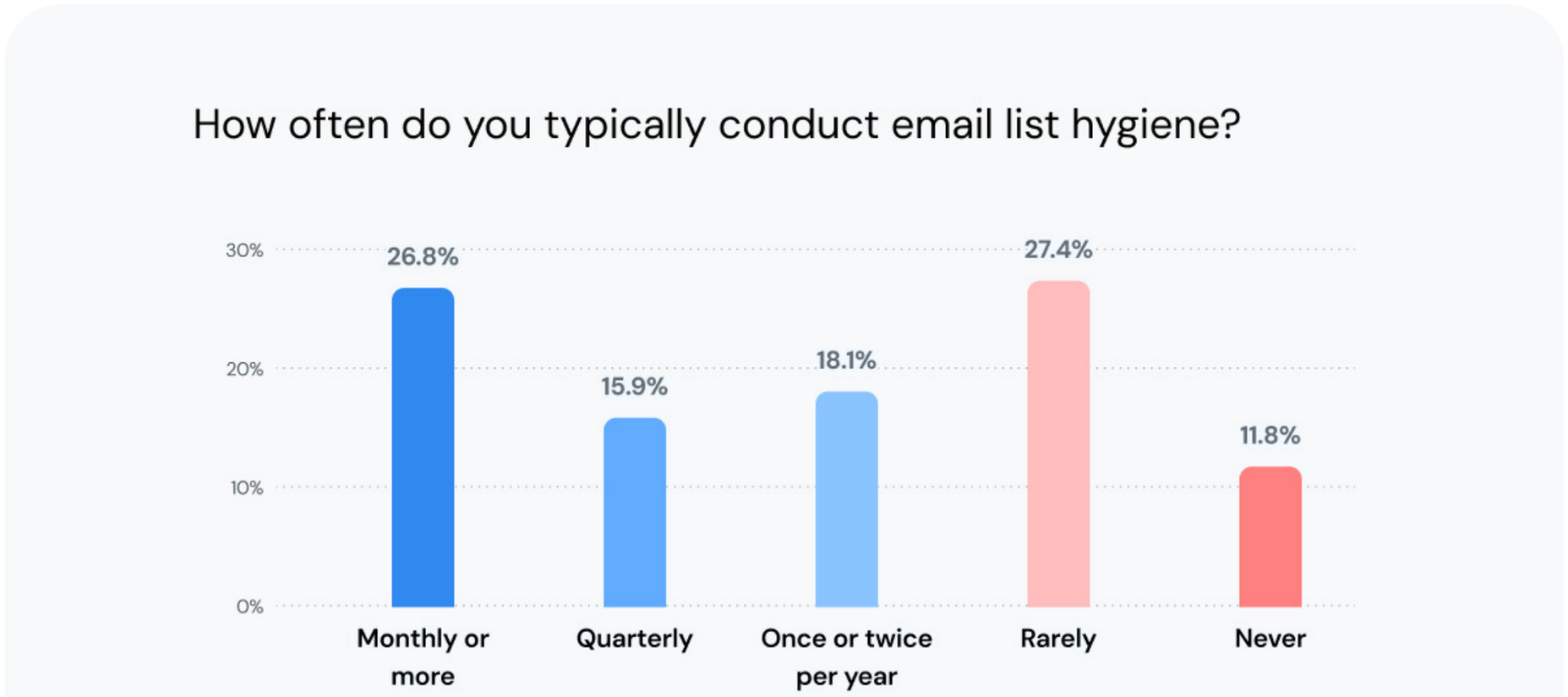
A compromise to the strict double opt-in method is something called **confirmed opt-in lite (COIL)**. This is when you only send certain emails to new subscribers, such as a welcome series or a monthly newsletter, until they engage. Once they do, you can add them to your main email list knowing they likely have a legitimate interest in what you offer.

Email list hygiene practices

You can get away with skipping a shower or two. Bathe once a week and maybe no one will notice. But try not showering for a month and see how people react when you walk into the room. When you have poor **email list hygiene**, it's mailbox providers who think you stink.

Here's what Sinch Mailgun's research reveals about how often senders conduct email list hygiene:

- 27% Monthly or more
- 27% Rarely
- 16% Quarterly
- 12% Never
- 18% Once or twice per year



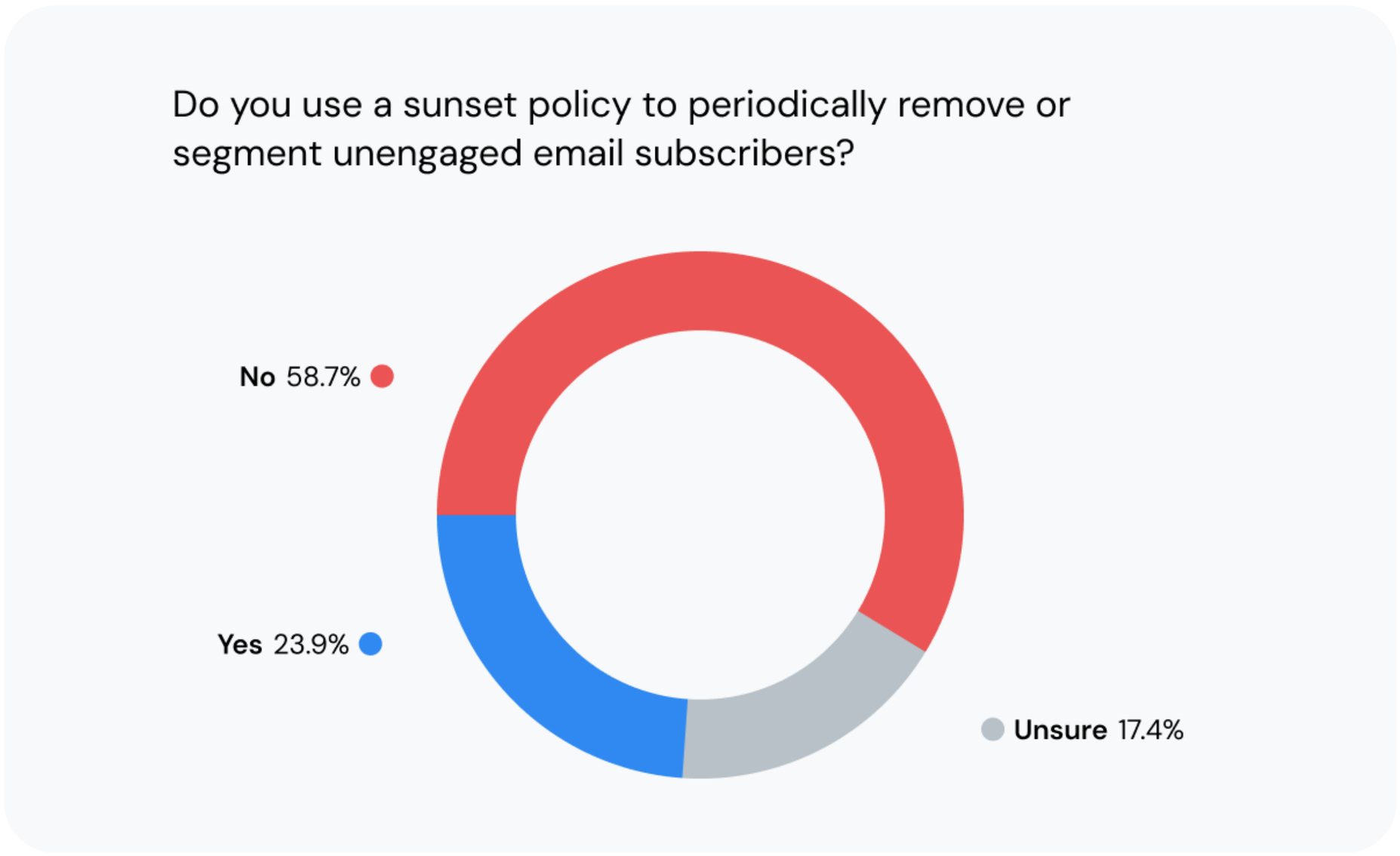
How often you need to conduct list hygiene depends on your list and the rate of growth. But if you're among **the nearly 40% who rarely or never conduct list hygiene,** you're putting your email communication efforts at risk of deliverability problems.

Here are some of the most common list cleaning tactics:

1. Remove contacts with hard bounces.
2. Unsubscribe contacts who make spam complaints.
3. Segment your list based on engagement levels.
4. Quarantine inactive subscribers (send to them less frequently).

One of the most effective ways to manage your email list is to **implement a sunset policy**. This involves setting specific thresholds or benchmarks for segmenting unengaged subscribers. For example, if someone hasn't opened an email from you in three months, that contact is "sunsetted" or moved off the main list.

Our research found sunset policies are uncommon among typical email senders. **Just under 24% of all senders use a sunset policy.** Nearly 59% say they do not and about 17% are unsure. These findings are almost unchanged from what we found in our 2023 survey.



Sunset policy implementation increases significantly based on email send volumes:

50%

Senders with 1 million+ monthly email volumes using a sunset policy.

34%

Senders with 100k to 1 million monthly email volumes using a sunset policy.

24%

Senders with 50k to 100k monthly email volumes using a sunset policy.

17%

Senders with < 50k monthly email volumes using a sunset policy.

These findings suggest tactics that help senders proactively manage list hygiene become more important as their contact databases grow.

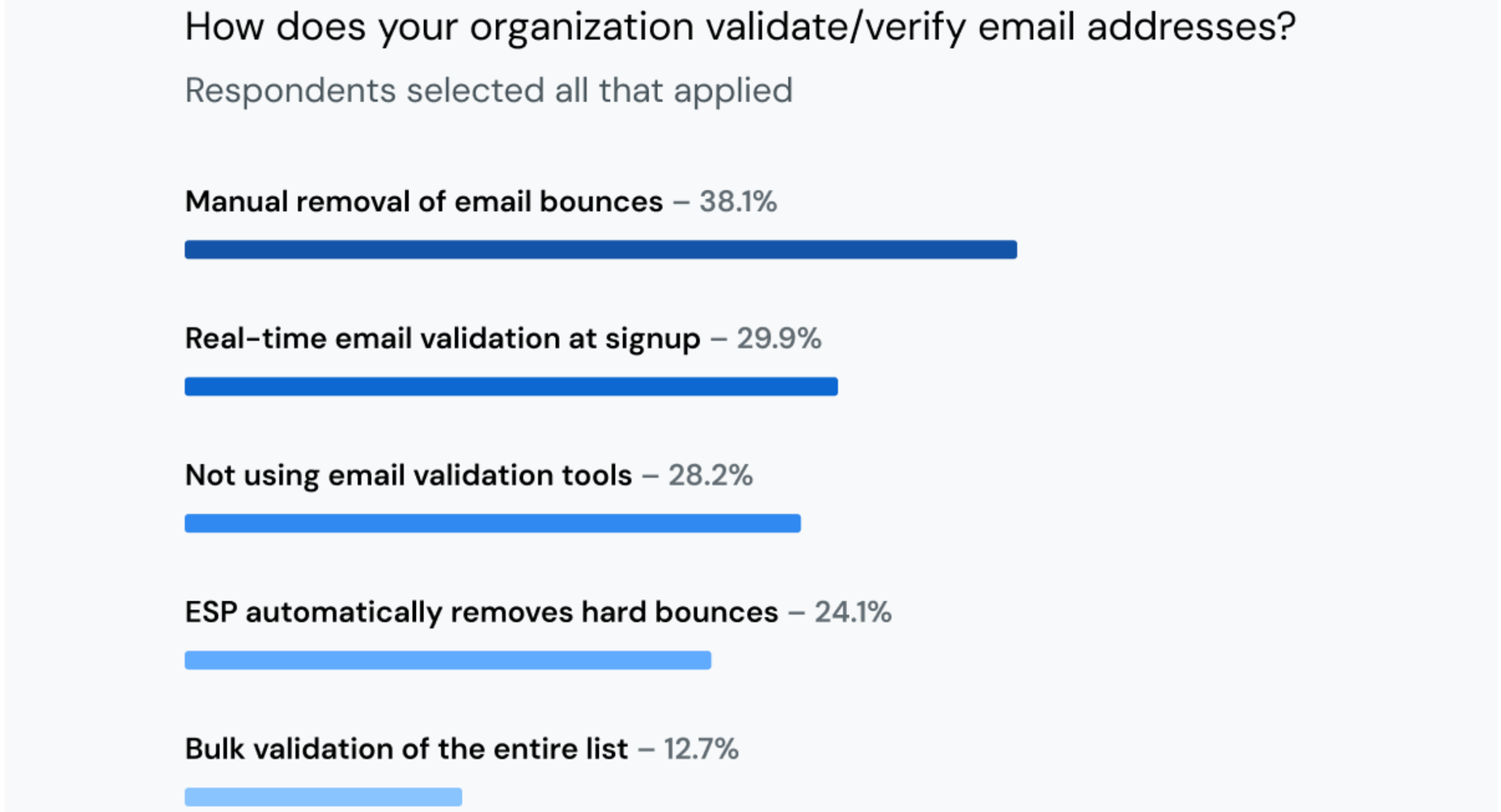
How email validation tools can help

Another way to proactively manage list hygiene is to **validate emails at signup** before you add them to your database. People make typos when filling out forms, like entering gnail.com instead of gmail.com. But you can help them correct those mistakes, so you don't lose out on new contacts.

The process of email validation does more than catch typos. It also verifies that an address can accept mail, it checks syntax for correct formatting, identifies disposable emails, and catches high risk email addresses. For B2B senders, it can even identify if a contact's domain (name@company-domain.com) is connected to a Gmail or Microsoft account.

Senders may verify emails at signup, and they can conduct bulk email validation on an entire database as part of regularly scheduled list hygiene. Both these methods are useful for maintaining a quality email list. One keeps bad contact data from getting on your list, the other helps you clean up the data that's already there.

We asked senders to identify the ways they validate emails. **30% conduct email validation at signup and almost 13% use bulk validation (only 3% do both).** 38% are manually removing hard bounces and 24% say their ESP does this automatically. 28% say they aren't using anything to validate emails.



Email validation also helps senders reduce bounce rates and maintain good engagement metrics. If you have invalid or outdated contacts in your database, they're not engaging with what you send, and that will drag your metrics down. List hygiene leads to a clear picture of email program performance.

CHAPTER 5

Email sender reputation

Mailbox providers are judging you – sizing you up as a sender and deciding if your emails are inbox worthy or deserve to end up in spam. Your goal is to stay on their good side, which means thinking about your email sender reputation.

Sender reputation is often compared to a credit score. Mailbox providers like Gmail and Outlook pay attention to your sending practices and use sophisticated algorithms to assess your reputation. Are you trustworthy? Are your messages anticipated and important? Or would "junk" be an accurate way to describe what's being sent?

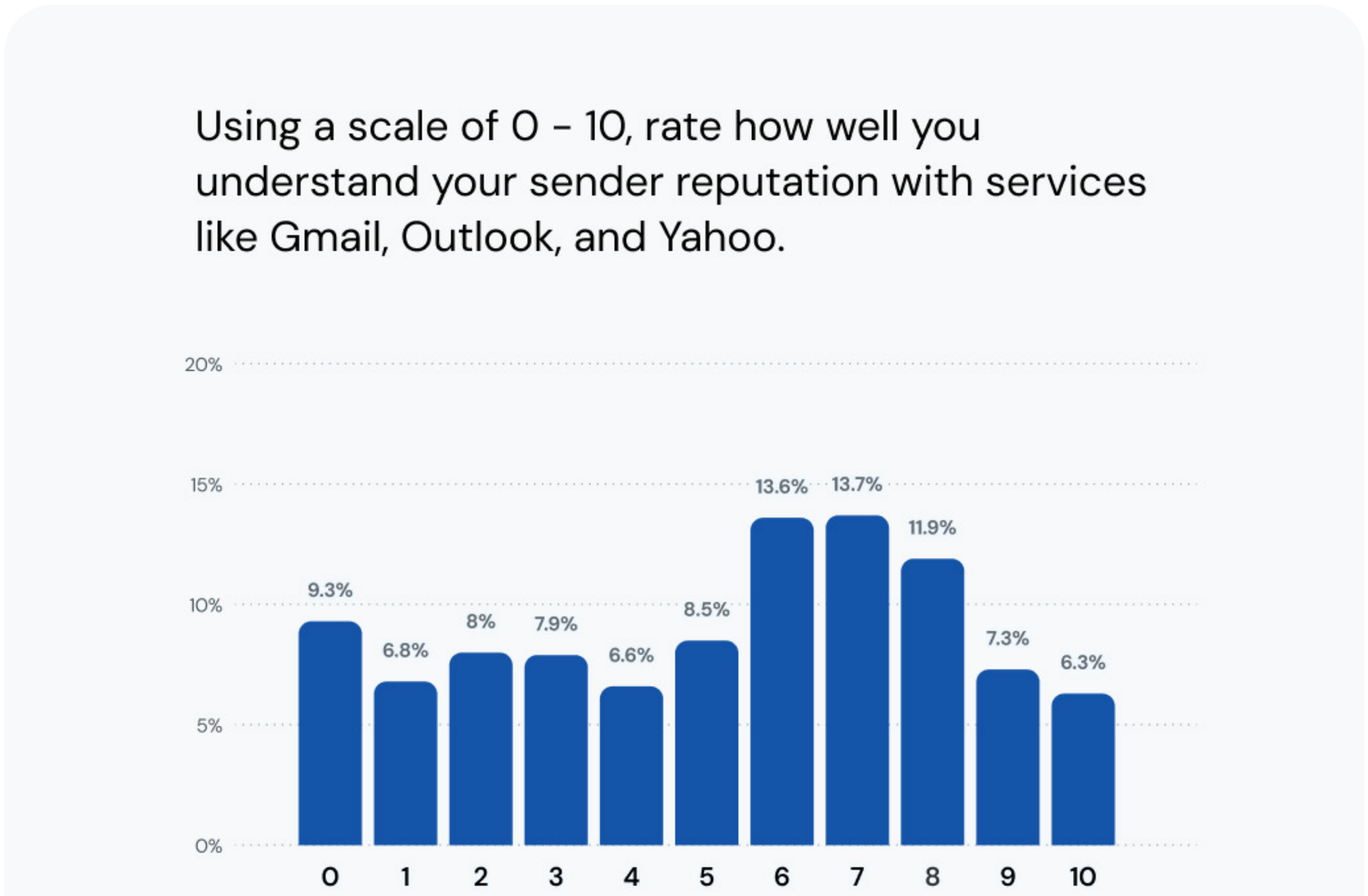
What's your sender reputation score?

Your email sender reputation includes these factors:

- IP and domain reputation
- Email authentication practices
- Sending patterns/consistency
- Positive and negative subscriber activities
- List quality
- And more...

While senders may have knowledge of these things individually, mailbox providers have their own ways of compiling multiple factors into a unique sender reputation score. Unlike a credit score, however, you won't be able to see your exact number with Gmail, Yahoo, or Outlook.

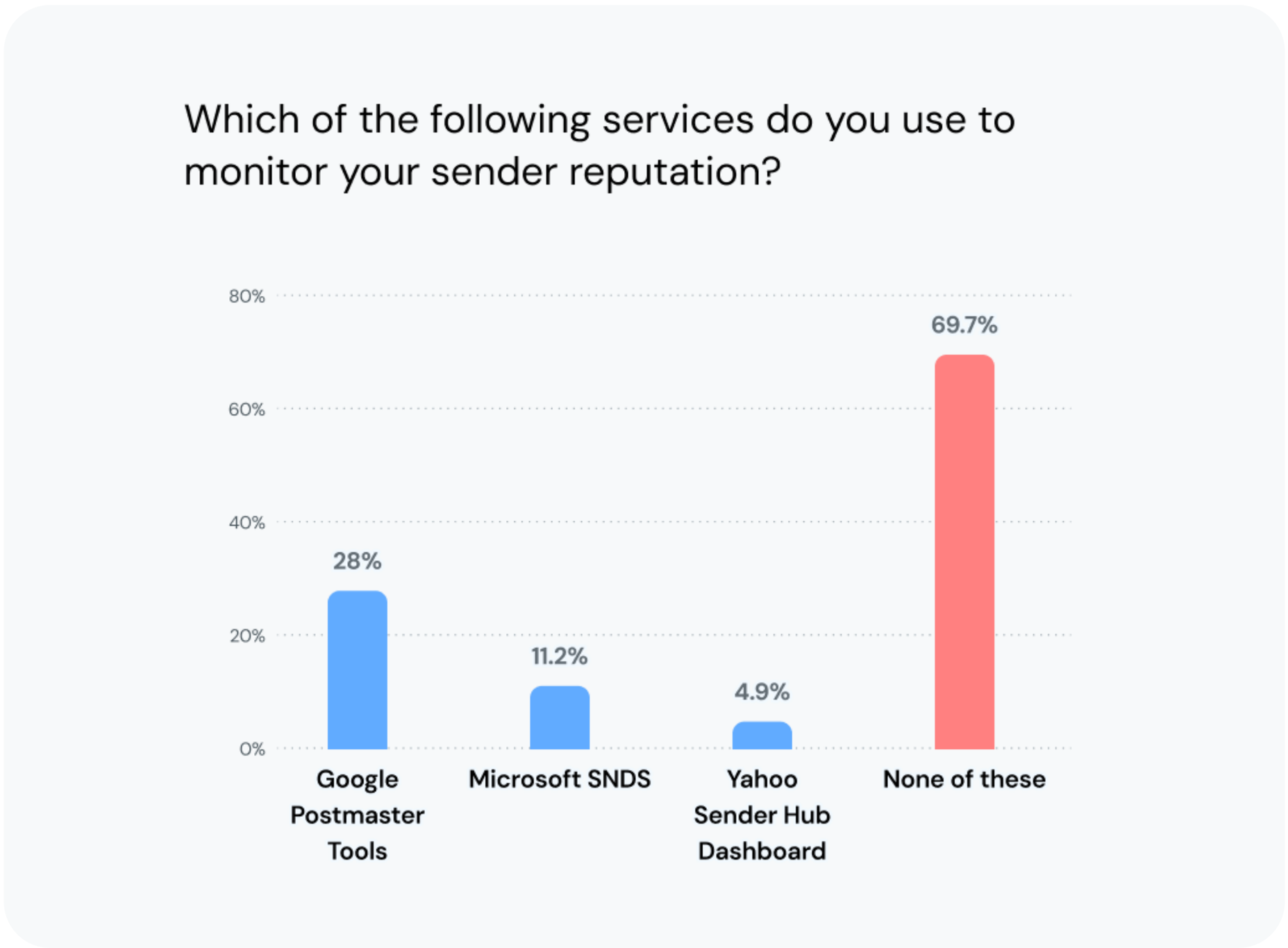
When we asked senders to rate their understanding of sender reputation on a scale of 0 to 10, 25.5% claimed to have a high understanding (8 to 10). **More than 42% of senders rated their understanding of sender reputation in the middle (4 to 7) and 32% rated it low (0 to 3).**



Since multiple factors contribute to your reputation, and individual providers have their own algorithms for scoring, it's easy to see why an accurate assessment is tough to come by. High volume senders were the most likely to rate their understanding of sender reputation as strong. That could be because they've identified the right tools to help.

While Gmail, Outlook, and others may not publish sender reputation scores, there are services that help you keep track of the factors that influence them. That includes **Google Postmaster Tools** for the Gmail ecosystem, **Microsoft SNDS** for Outlook, and the **Yahoo Sender Hub**.

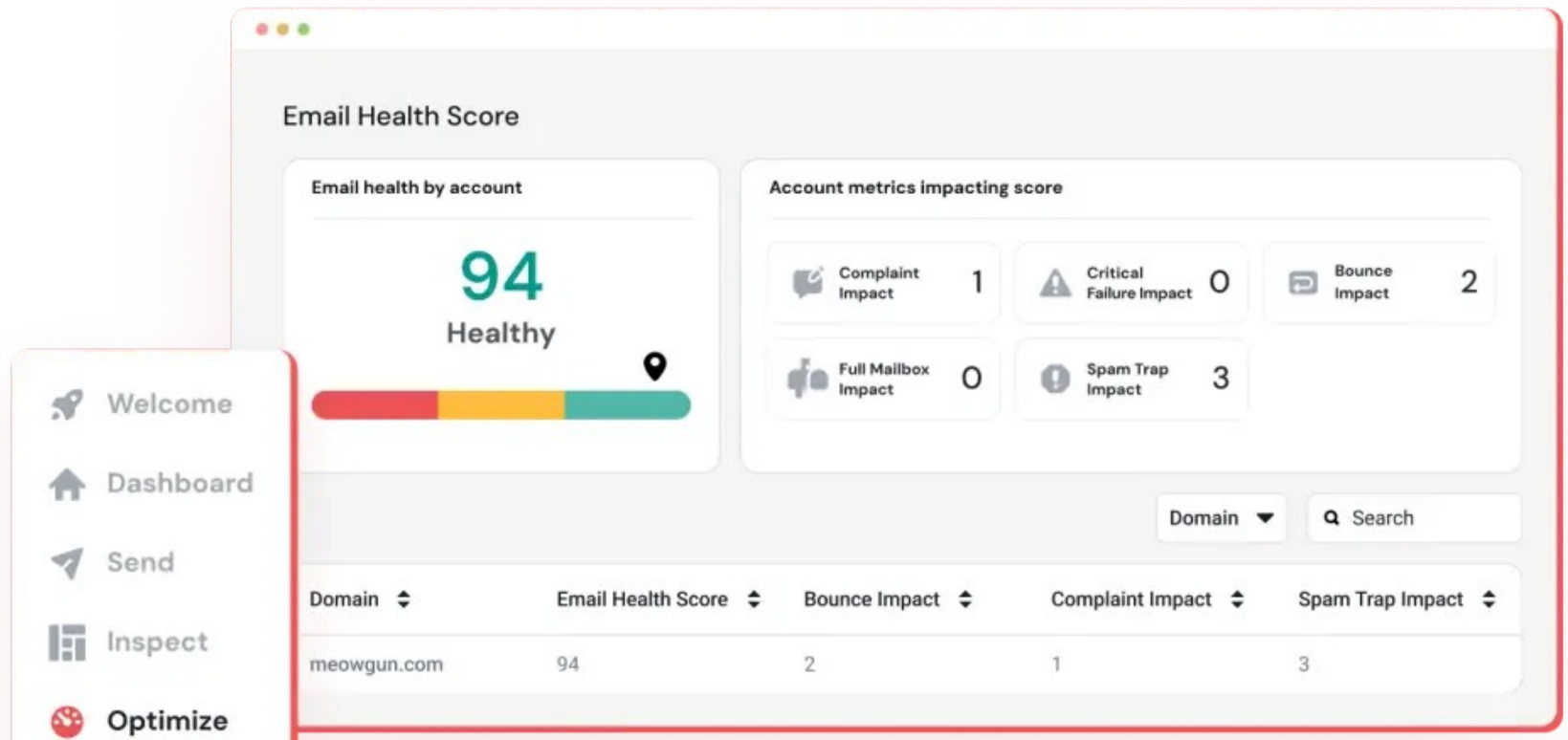
However, when we asked senders in our survey if they use these services, adoption was quite low. **Nearly 70% of respondents are not using any of the three services from major mailbox providers to monitor sender reputation.** The most used was Google Postmaster Tools at 28%.



Use of these services is much more common among the highest volume senders. More than 63% of those sending over one million emails per month use Postmaster Tools while nearly one-third use Microsoft SNDS. Just over 11% of the largest senders use Yahoo's service, which is newer in comparison and is adding features for senders.

A key feature each of these services offers is a complaint feedback loop (CFL). This is a system that notifies senders when recipients mark emails as spam. The notifications contain specific information about complaints so the sender can address the situation. That could mean removing addresses that complain, adjusting sending frequency, or changing email content.

Postmaster Tools and SNDS also offer information on IP and domain reputation as well as email authentication, delivery errors, and more.



EMAIL DELIVERABILITY TOOL

Uncover sender reputation insights

Mailgun Optimize offers integrations with both Google Postmaster Tools and Microsoft SNDS so senders can easily monitor their reputations. The platform also provides an **email health score** based on five critical signals that contribute to your reputation, giving you a snapshot of overall email deliverability.

Get reputation monitoring

IP reputation and domain reputation

The foundation of sender reputation involves your sending domains and the IP addresses from which emails are sent. So, decisions concerning your email sending infrastructure can impact deliverability.

In general, your **domain reputation reflects the history of your organization's digital trustworthiness.** In a way, it's connected to brand reputation. Your **IP reputation reflects recent sending practices,** and it may be shared with others on the same sending IP.

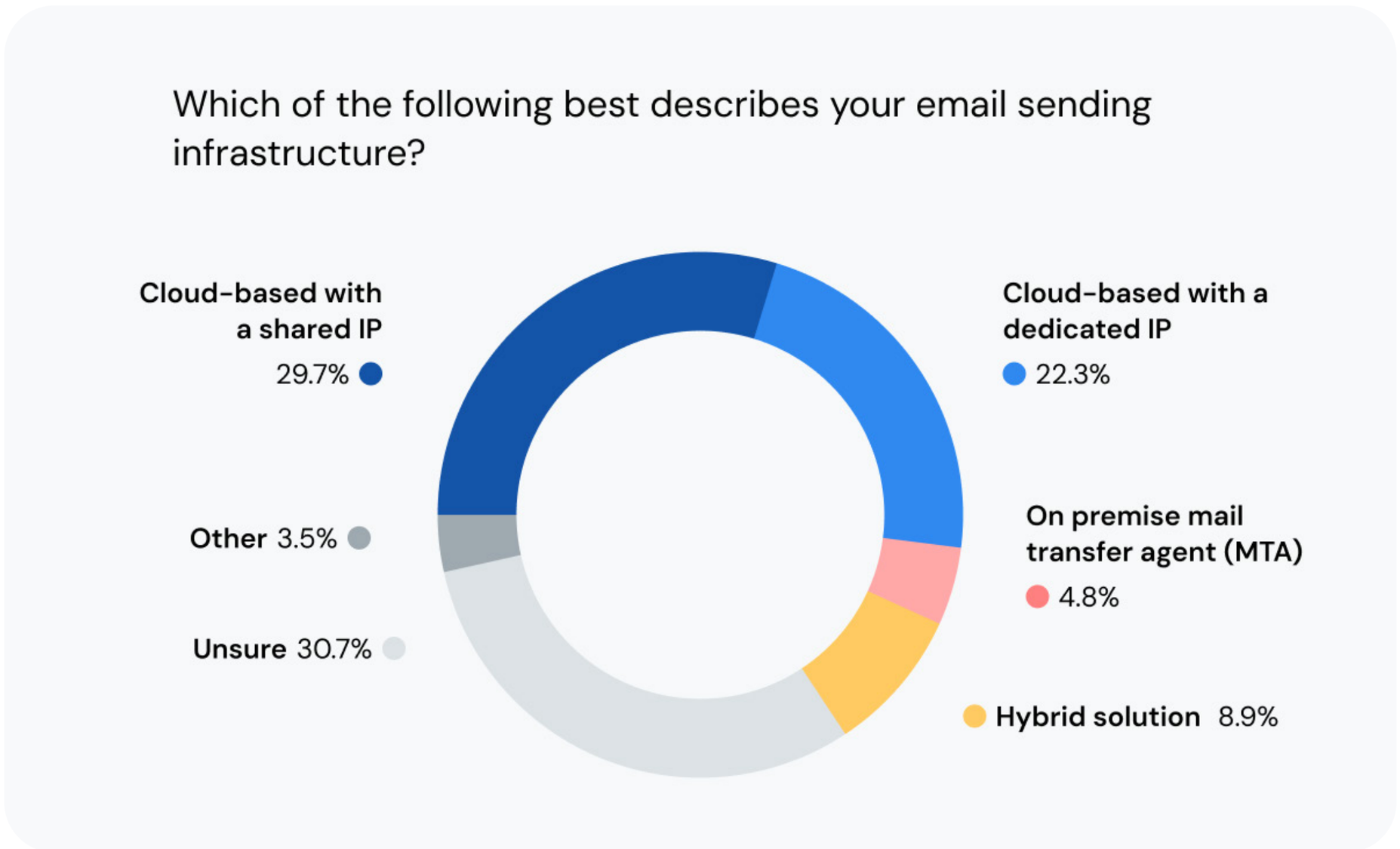
Email sending IPs

Emails can be sent from either dedicated or shared IP addresses. The reputation of a dedicated IP belongs to just one sender. **On a shared IP, the behavior of other senders using the same IP address could impact your deliverability.** That's why it's important to choose an email service provider (ESP) that closely monitors who is using the platform.

For example, **Sinch Mailgun's Acceptable Use Policy (AUP)** is designed to keep senders responsible. First, certain types of senders and email content are prohibited. Sinch Mailgun users must also stay below defined thresholds for bounce rates, spam complaints, unsubscribes, and blocks. That's what protects legitimate senders on our shared IPs from being impacted by bad actors. Everyone strives for a good sender reputation.

Our survey shows cloud-based email infrastructure solutions are most common, with **a combined 52% of all respondents saying they use cloud-based email infrastructure.** Only 5% of respondents said they use on-premises infrastructure and 9% have a hybrid solution.

Cloud-based email infrastructure solutions typically offer both dedicated and shared IPs. Nearly 30% of them have a shared IP while 22% are using a dedicated IP.



Nearly 31% of senders were unsure of their email infrastructure while just under 5% have it on premises and 9% use a hybrid solution.

A **dedicated IP** is more common among high volume email senders, and our survey shows that. 45% of respondents with volumes greater than one million emails per month have a dedicated IP compared to just 15% of those sending fewer than 50,000 emails per month.

Sinch Mailgun recommends a minimum volume of 100,000 emails per month for dedicated IPs. For many senders, a shared IP will work just fine. Find out more about the differences between **dedicated and shared IPs** for email sending.

Email sending domains

When a sender has deliverability issues with an IP, switching to a new one can sometimes be a solution. Although, if bad habits continue on the new IP, their bad reputation will quickly catch up with them. **Domain reputation follows you wherever you go.**

Domain reputation is based on the history of a sending domain's trustworthiness. Some factors connected to domain reputation you can control, such as the DNS records used for email authentication. Others, such as the age of your domain, are out of your control.

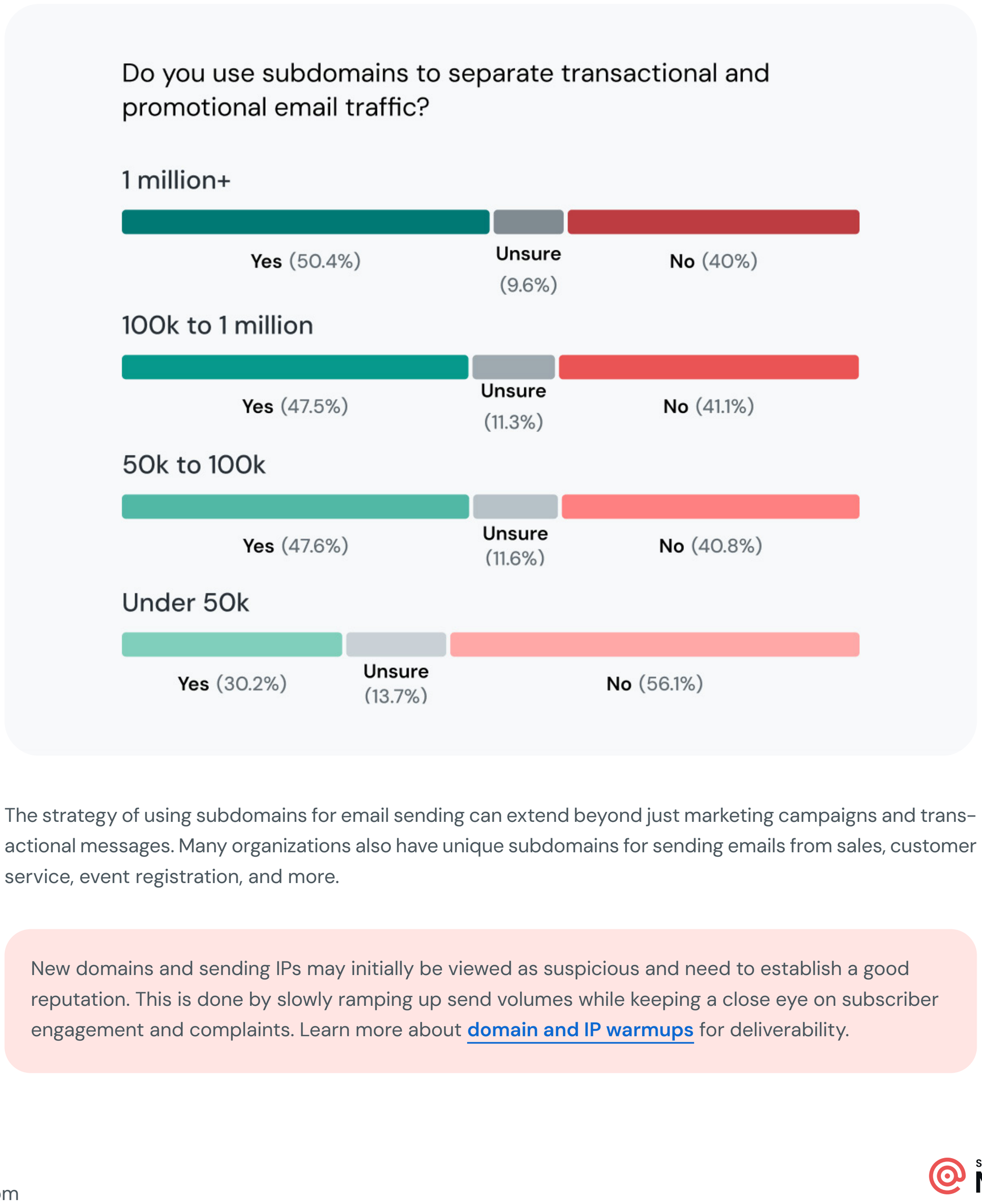
An effective way to use domains to support inbox placement is to separate your mail streams. This is often done by sending promotional and transactional emails from different subdomains.

For example, email campaigns and newsletters come from marketing.yourcompany.com while transactional messages are sent from orders.yourcompany.com. Transactional emails are much less likely to be marked as spam since they are expected and highly relevant. It's also important that transactional messages avoid the spam folder as they usually contain timely information recipients want and expect.

If all your emails came from the root domain and people started marking promotions as spam, that could negatively impact deliverability of transactional messages. **Using different subdomains for promotional and transactional emails helps distinguish different domain reputation for those mail streams.**

Find out more about domain reputation and when to use an email subdomain to help you establish email infrastructure that's optimized for inbox placement.

Sinch Mailgun research found the practice of using separate subdomains for email sending is fairly common, especially among higher volume senders. **Nearly 50% of senders with volumes greater than 50,000 emails per month are separating marketing and transactional messages on different subdomains.** However, 30% of the lowest volume senders also implement this practice.



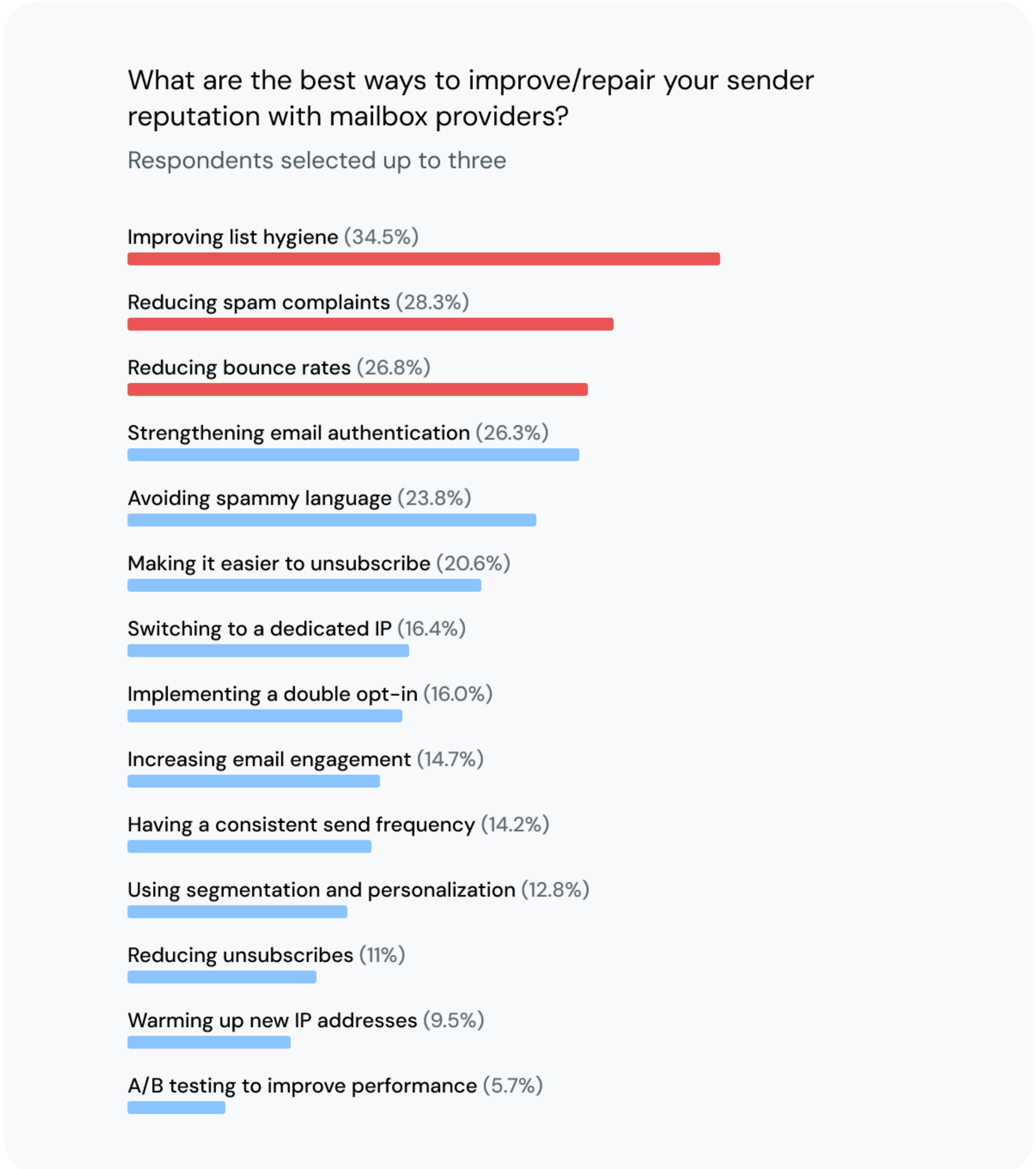
The strategy of using subdomains for email sending can extend beyond just marketing campaigns and transactional messages. Many organizations also have unique subdomains for sending emails from sales, customer service, event registration, and more.

New domains and sending IPs may initially be viewed as suspicious and need to establish a good reputation. This is done by slowly ramping up send volumes while keeping a close eye on subscriber engagement and complaints. Learn more about **domain and IP warmups** for deliverability.

How to improve email sender reputation

Beyond the reputation of domains and IPs, what can you do to send the right signals to mailbox providers? There are plenty of different levers you can pull to make sure your email program is viewed positively. We asked senders to choose three they believe are best for improving sender reputation.

The most popular answer was **Improving list hygiene** (34.5%). That's followed by **Reducing spam complaints** (28.3%) in the second spot while more than 26% each chose **Reducing bounce rates** and **Strengthening email authentication.**



Selections were spread widely among the options. The truth is, all these efforts can **improve sender reputation** or help you avoid problems that could damage it. What works best will depend on your email program's current state and where there's room for improvement.

It's good to know why certain activities support your email sender reputation. For example, the idea of **avoiding spammy language is a bit of a deliverability myth.** Putting the word "free" in a subject line or occasionally using ALL CAPS probably won't get you filtered into junk folders.

This may have been true in the past. However, modern spam filters are much better at identifying spam using other factors. It may be hard to compose copy for certain campaigns without using so-called "**spam trigger words.**" Plus, these days, phishing scams are just as likely to spoof transactional emails such as shipping delays or other notifications.

A better reason to avoid using spammy language in emails is because recipients, not mailbox providers, may feel like you're spamming them. That can prompt them to mark an email as spam, and a high spam complaint rate will hurt deliverability.

> If you're focused on spammy language but you still haven't implemented DMARC, you need to get your email deliverability priorities straight. Mailbox providers are much more likely to filter unauthenticated email into spam. Find out how to **set up DMARC** in five steps.

Email engagement and sender reputation

When we asked senders about the best ways to improve their reputation in 2023, email engagement was the top answer. While more than 25% chose **Increasing engagement** in our 2023 report, less than 15% did so this time.

On the other hand, we saw spikes in perceived importance for other factors that can impact email sender reputation and deliverability. For example, only 1.6% of respondents chose **Making it easier to unsubscribe** in 2023, but 20.6% chose it in our most recent survey.

The impact of new sender requirements from Google and Yahoo in 2024 may explain these year-over-year differences. The changes brought awareness to email authentication, spam complaint rates, and an easy one-click unsubscribe process.

2023

25.4%

Senders who selected **Increased engagement** in 2023

1.6%

Senders who selected **Making it easy to unsubscribe** in 2023

2024

14.7%

Senders who selected **Increased engagement** in 2024

20.6%

Senders who selected **Making it easy to unsubscribe** in 2024

While it's good to see more attention in these areas, senders shouldn't lose sight of the importance of email engagement and how it relates to sender reputation. Engagement is a measurable factor you can work to continuously improve, especially through email marketing efforts.

The more that people open, read, click, respond to, and forward your messages, the more apparent it is to mailbox providers that your campaigns belong in the inbox. On the other hand, if your emails are being ignored, deleted, or people are unsubscribing in droves, mailbox providers will assume you belong in the junk folder.

12.8% of senders chose personalization and segmentation as a tactic to improve their sender reputation score. 5.8% picked A/B testing. Even though these options landed lower on the list, they can also help you improve your engagement metrics to boost sender reputation. Segmentation and personalization lead to more relevant emails, and A/B testing helps you discover what your subscribers are most likely to engage with.

In the end, it's all connected. Cleaning up your email list to remove inactive subscribers and sending more personalized, targeted emails results in higher email engagement rates. Making it easy to unsubscribe removes people who don't want your emails from the equation as well.

CHAPTER 6

How to improve email deliverability

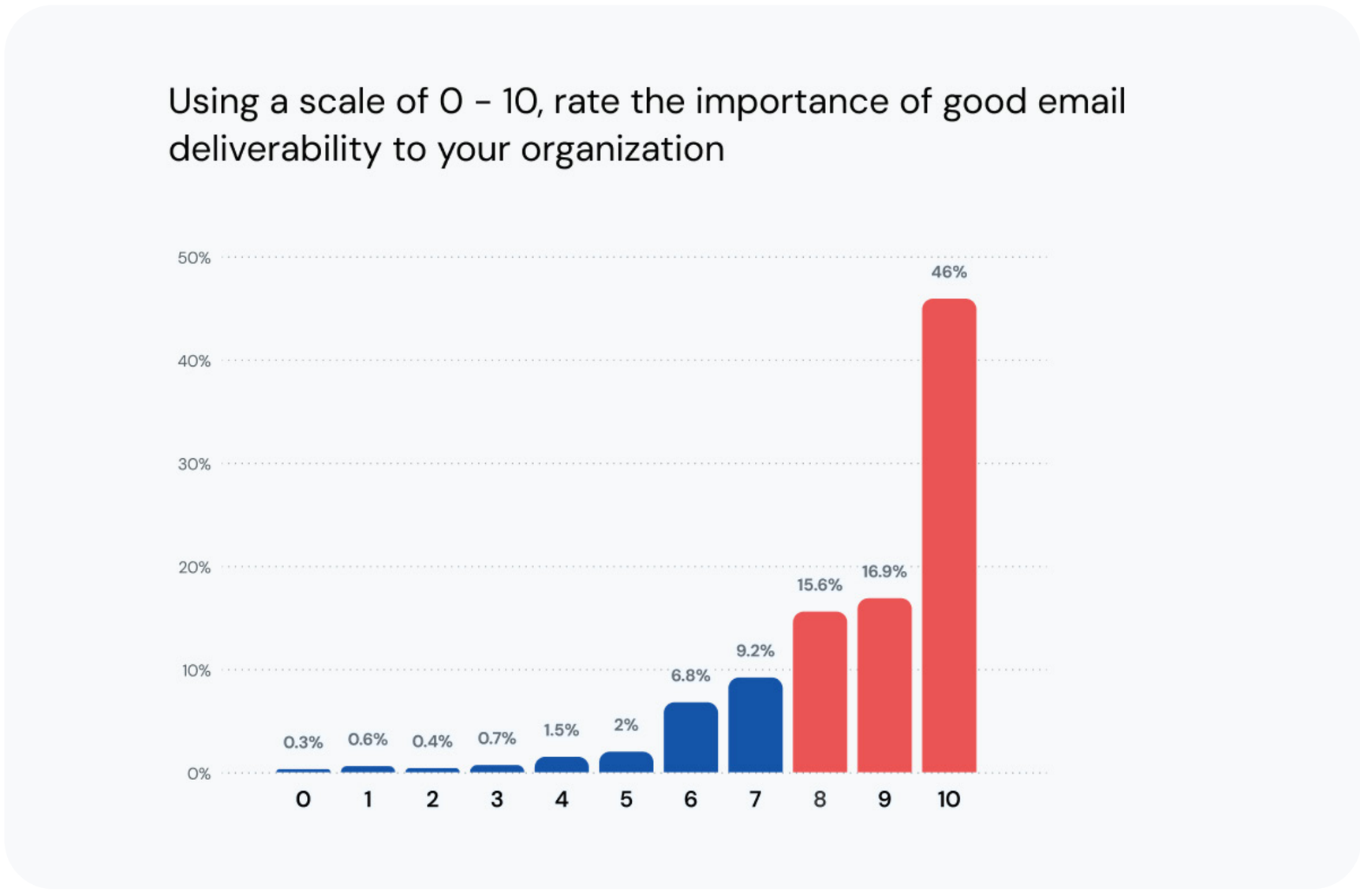
Email is a very dependable channel for marketing and communications in many organizations. It’s easy to dismiss the need to improve email deliverability because you may simply expect everything to work. But what if delivery of your emails was disrupted? How would that impact day-to-day aspects of the business?

Deliverability is a lot like personal health. You can wait for problems to show up and address the symptoms, or you can take preventive steps to stay in good shape.

Let’s wrap up Sinch Mailgun’s State of email deliverability 2025 with some insights into the importance of deliverability and reminders to help you stay on the right side of the inbox.

The importance of reaching the inbox

We asked senders to rate the importance of achieving good email deliverability from 1 to 10. It’s clear that most see it as a priority. **78.5% of respondents rated the importance of email deliverability between 8 and 10. In fact, 46% gave it a solid 10.** We’d say that’s pretty important.



The size of the organization and the volume of email had little to do with the level of perceived importance. But if reaching the inbox is so vital, many senders could do more to improve deliverability.

Consider these key findings from Sinch Mailgun's original research:

87%

of senders do not use inbox placement testing to measure deliverability.

70%

of senders are not monitoring their reputation with Google Postmaster Tools.

53%

of senders do not actively monitor major email blocklists for their IP/domain.

39%

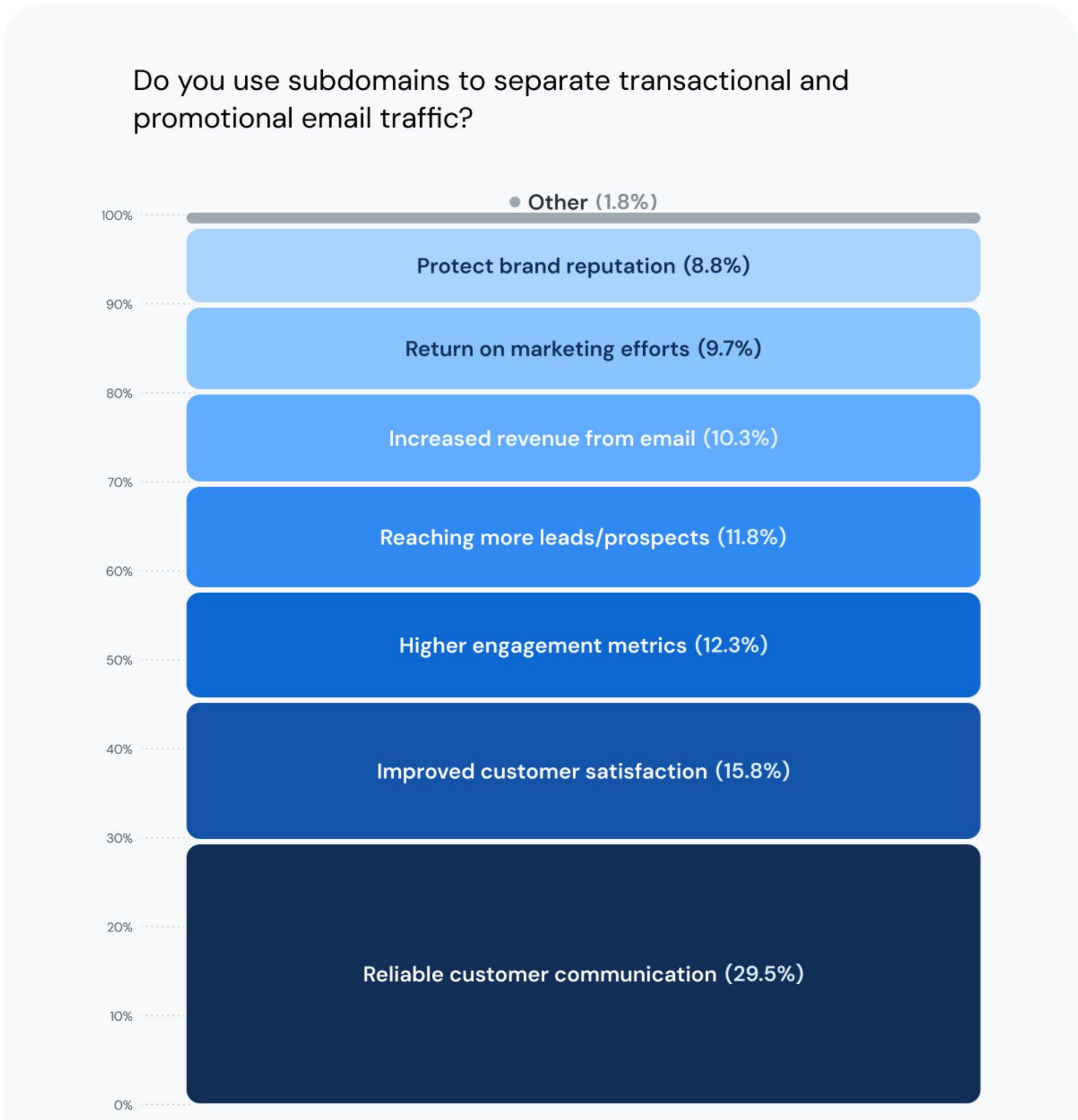
of senders rarely or never conduct email list hygiene.

Is your organization one that needs to step up its investment in email? How much more effective could this channel be if you worked to improve email deliverability?

The benefits of prioritizing deliverability

Need some good reasons to put deliverability higher on your priority list? We asked senders who rated the importance of deliverability highly about the biggest benefits of achieving inbox placement.

Two factors related to the customer experience emerged as most beneficial: **Reliable customer communication** (29.5%) and **Improved customer satisfaction** (15.8%).

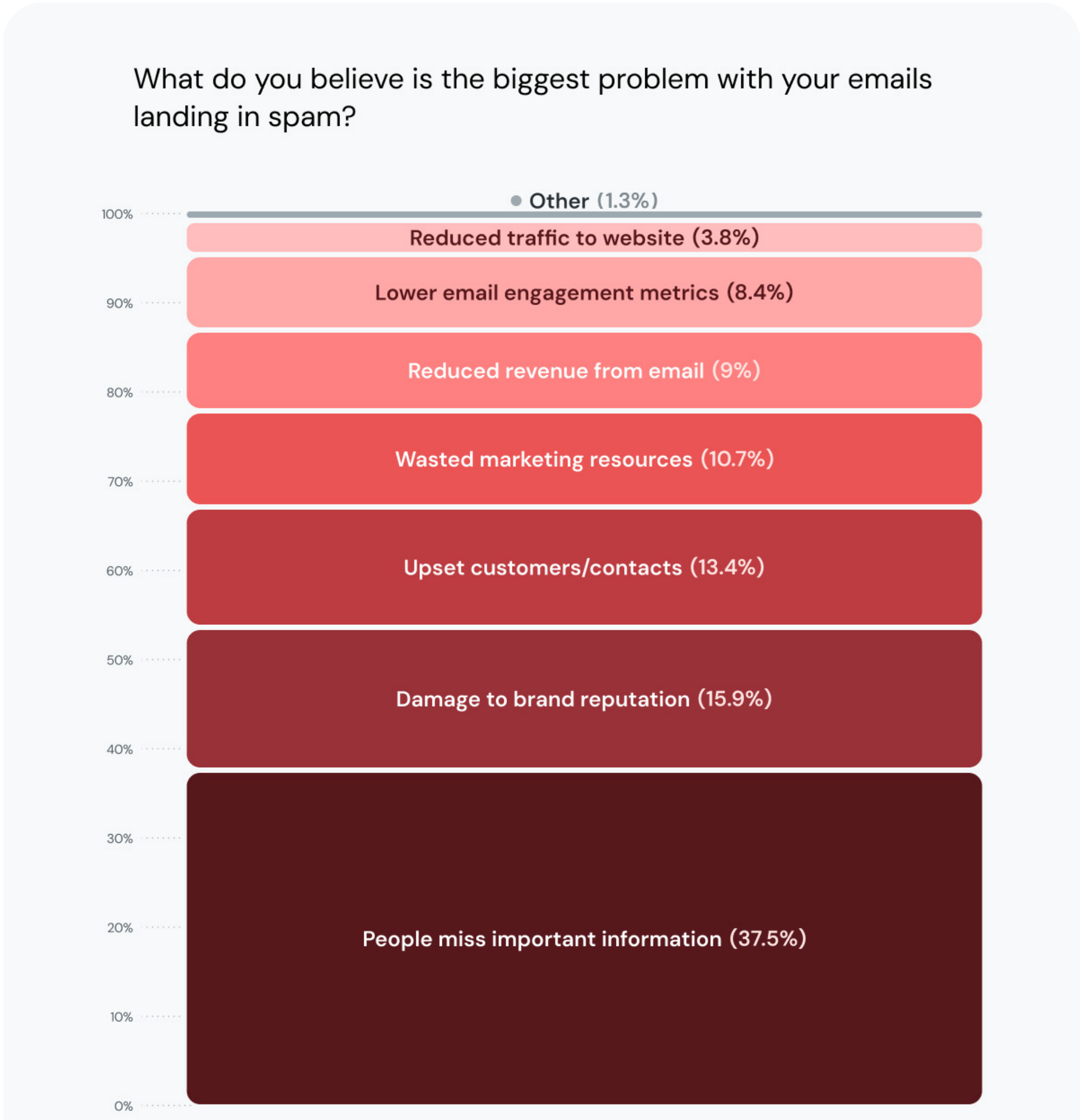


Around 10% of senders believe the biggest benefit of good deliverability is **Increased revenue from email,** and about the same percentage feel that way about getting a **Return on marketing efforts** (9.7%).

This makes a lot of sense for email marketers. You can't boost sales with promotional emails if they fail to reach the inbox. And while the **ROI of email** is notably high, that's only true when your messages reach subscribers.

Transactional emails may not drive revenue, but they are just as important as any marketing campaign. **Sinch Mailgun research** found **71% of consumers would check their spam folder if a transactional message didn't show up in their inbox**. (Another 16% would check spam if the message was important.)

But ending up in junk is not a good look. That's like making your subscribers dig through a garbage bin for a piece of missing mail. As we've noted, this can cause contacts to lose trust or unsubscribe. When we asked senders to choose the biggest problem with landing in spam, **Damage to brand reputation** (15.9%) was second only to **People miss important information** (37.5%).



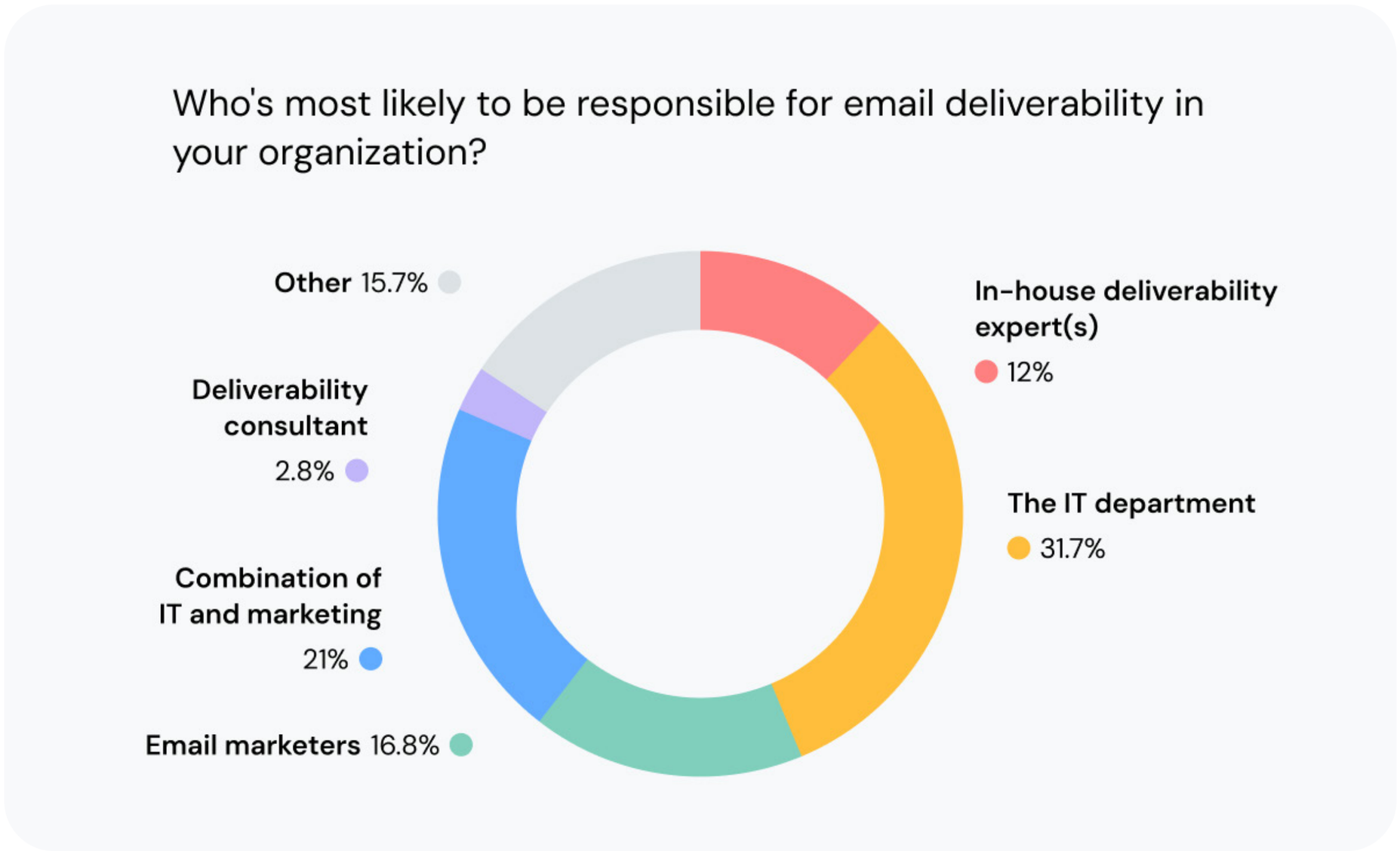
Upset customers/contacts (13.4%) took the third spot. And as with the benefits of good deliverability, around 10% of senders cited reduced revenue and wasted marketing resources as downsides of landing in spam.

Who is responsible for email deliverability?

The people who took our survey come from a wide range of industries and job roles. Respondents included small business owners and C-suite executives as well as marketers, software developers, IT professionals, and deliverability specialists.

Achieving inbox placement requires technical knowledge as well as marketing expertise. You need people who understand DNS TXT records for authentication as well as those who understand the target audience.

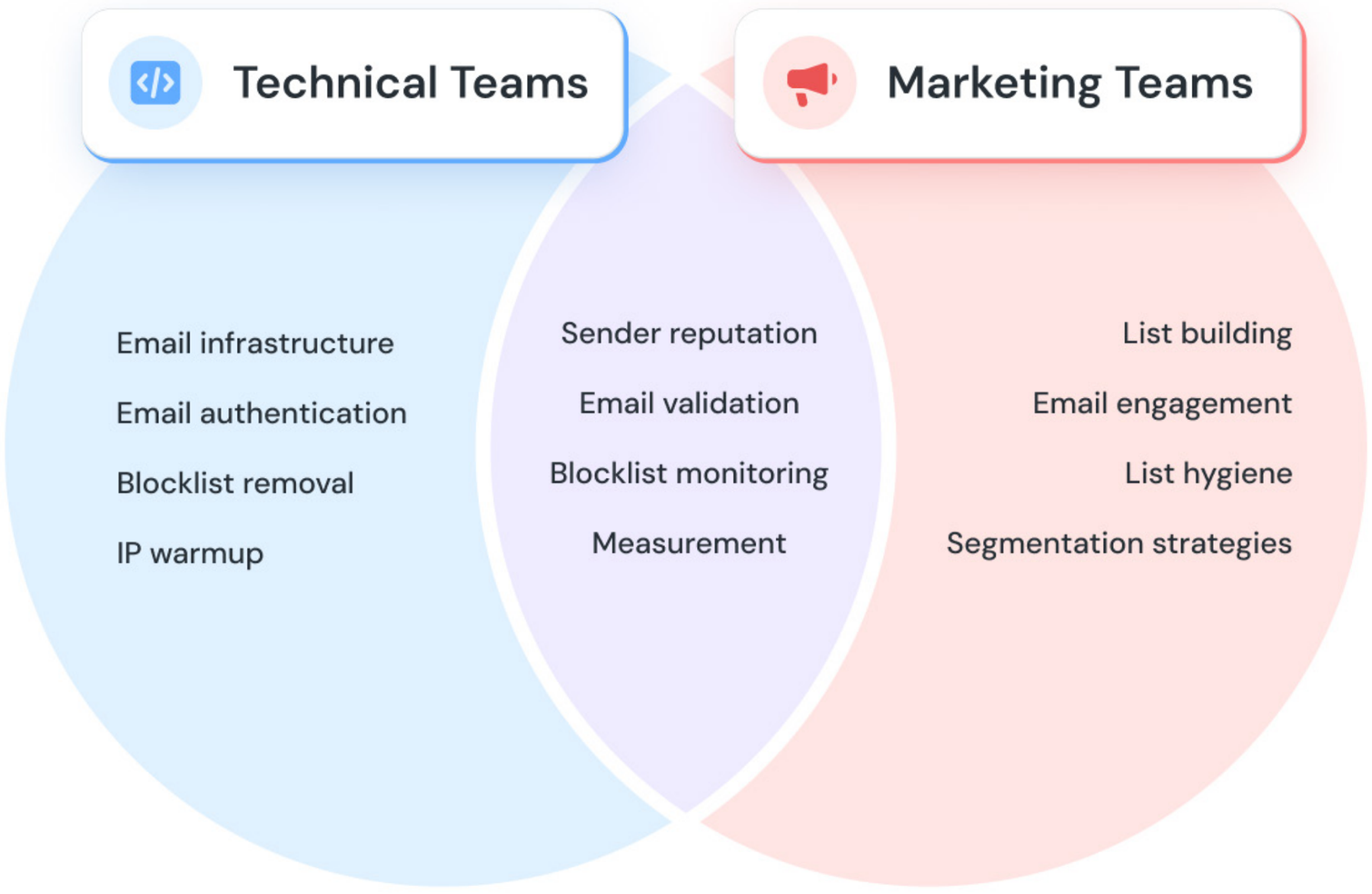
Our survey found that 31.7% of respondents say the IT department is responsible for deliverability in their organization. 16.7% said responsibility for inbox placement falls to the marketing team. **But more than 20% understand that it takes both technical and marketing team members to support email deliverability.**



12% of respondents told us they employ in-house deliverability experts while just under 3% are working with a deliverability consultant. However, even when you have people dedicated to deliverability, responsibility can still fall on the shoulders of other people throughout your company.

While initial setup from technical team members is crucial to deliverability, the way people in your organization use email to reach customers and prospects also impacts inbox placement. That's why improving deliverability does include both technical and marketing efforts. Some tasks are a combined effort.

Email deliverability responsibilities



All our survey respondents are somehow involved with email in their organizations, but only around 5% described their job as being an “Email deliverability specialist.” Most of the respondents with in-house deliverability specialists come from larger organizations. It is a niche position, but the need and demand for it could be growing.

How to improve email deliverability and sender reputation

There are dozens if not hundreds of factors that impact inbox placement. To help you wrap your head around it all, let’s focus on four key areas to help you improve email deliverability.

1. Email infrastructure and technology

Deliverability begins with the systems, tools, and processes used to send email. When technical teams make email infrastructure decisions, it involves sending domains and IP addresses as well as whether to separate mail streams. You’ll also decide whether traditional SMTP or integrating sending with an email API is better for your needs.

There are other technology partner choices too, such as finding a reliable email service provider (ESP) and

tools to help measure, monitor, and maintain deliverability.

Key findings from the report

- **Cloud-based email infrastructure** is most common:
  - 29.7% Cloud-based with a shared IP
  - 22.3% Cloud-based with a dedicated IP
  - 30.7% Unsure about email infrastructure
- Just over 50% of the highest volume senders **separate mail streams** on different subdomains.

Deliverability tips

- **Sending more than 100,000 emails a month?**
  Consider a dedicated IP for more control over your sender reputation.
- **Using a shared IP?** Protect your reputation and make sure your provider has rules to keep bad senders off the platform.
- **Sending all messages from the same domain?** Look into separating promotional and transactional emails on subdomains.

★

Resources on infrastructure and technology

- SMTP vs email API: Their differences and how to use them
- Which SMTP port should you use?
- Preparing your email infrastructure
- Dedicated vs. shared IPs: Know which one to use
- The basics of email subdomains and how to use them

2. Email authentication

Without proper authentication protocols in place, you’ll have a very hard time reaching inboxes. Plus, a lack of authentication puts your emails at risk of spoofing. While email authentication may be the most technical of all email deliverability factors, it’s worth the time and effort to get it right.

The new sender rules from Gmail and Yahoo require all senders to use SPF or DKIM. If you send mass emails regularly, you need to use SPF, DKIM, and DMARC.

Key findings from the report

- Nearly 80% of senders who were aware of new sender requirements in 2024 **updated their email authentication protocols.**
- More than 66% of senders **use both SPF and DKIM** for authentication.
  - 25.7% are unsure
- 53.8% of senders **use DMARC to support authentication** in 2024.
- 25.5% of senders using a p=none policy plan to **switch to a stronger DMARC policy** in the next year.

Deliverability tips

- **Want strong authentication and a good sender reputation?** Use all three protocols: SPF, DKIM, and DMARC.
- **Unsure how your organization authenticates email?** Check with your IT department, DNS provider, or ESP for answers.
- **Using a p=none DMARC policy?** It's a step in the right direction, but you'll need to switch to a policy of Reject or Quarantine to get the full benefit of DMARC.
- **Worried about authentication failures?** Make sure you understand email error codes and bounce classifications or use a **tool to test authentication configurations.**

Resources on email authentication

- **The basics of SPF records**
- **What is DKIM? How it works and why it's necessary**
- **How to implement DMARC: A step-by-step guide**

DOWNLOAD

Email authentication guide

Get technical advice on configuring your SPF, DKIM, and DMARC records from the team at Sinch Mailgun. Download this free, ungated guide to help you comply with sender requirements and make the email inbox a safer place.

Start authenticating

3. Email engagement levels

Once your email sending program is technically sound, it's often the activities of the marketing team that can damage or improve email deliverability. Getting recipients to engage with what's sent will impact inbox placement.

The actions your subscribers take send signals to mailbox providers about your email sender reputation. Too many spam complaints = Bad. Increasing opens and clicks = Good. That's easy to understand – but not always easy to accomplish.3. Email engagement levels

Key findings from the report

- 57.4% of senders **monitor opens and clicks** to help measure deliverability.
- Less than 15% of senders selected email engagement as a key factor that **improves sender reputation.**
- Only 24% of senders **use a sunset policy** to identify unengaged subscribers.

Deliverability tips

- **Want your emails to be more engaging?** Start using segmentation and personalization to make messages more relevant. Strategic segmentation can be based on engagement levels.
- **Need to improve email performance?** A/B test elements of email campaigns to discover what gets your recipients to engage.
- **Are you making it easy to unsubscribe?** Don't worry about unengaged contacts who want to stop getting your emails. Make sure they can unsubscribe in one click.
- **Trying to stay out of spam?** Keep your user reported spam complaint rate well below 0.3% (below 0.1% is best). Remove complainers from your list ASAP.

Resources on email engagement

- What is RFC 8058 for one-click unsubscribe?
- How to keep your spam complaint rate low
- Email metrics explained: Understanding email performance
- Sunset policies and email engagement: A complete guide
- How to promote strategic engagement in your email program

4. List building and hygiene

While you can't control how your subscribers engage with your emails, you can control how you manage your list. Good email engagement begins at signup.

Adding contacts to your list without getting explicit permission will not only hurt email engagement, but it could also get you in legal trouble. However, even subscribers who opted in will drag down engagement rates as they lose interest or abandon email accounts. That's why proactive list hygiene is vital

Key findings from the report

- More than 60% of senders **conduct list hygiene** at least once or twice per year.
    - 27% clean their lists monthly or more.
- Nearly 10% of senders have **purchased a list or scraped the web** for contacts in the last two years.
- Close to 40% of senders **use a double opt-in method** to confirm new contacts before adding them to their list.
- Around 28% of senders are not using any tools to **automate email validation.**

Deliverability tips

- **Did you get explicit consent?** Never add contacts to your email marketing list without permission. Transactional messages may be sent with implied consent.
- **Forgetting to think about list hygiene?** Set a regular cadence for conducting bulk validations and use a sunset policy to help quarantine inactive contacts.
- **Want to keep your database clean?** Be proactive about list hygiene and verify new contacts' emails before they're added to your list.
- **Are you sure they want your emails?** A double opt-in process confirms intent to subscribe, keeps bots off your list, and ensures new contacts are likely to engage.

Resources on email list hygiene

- How to build an email list the right way
- Explicit consent and the GDPR
- Email list management best practices
- Why email list management matters
- Email validation: Why is it vital for deliverability?

Final thoughts on improving email deliverability in 2025

Sinch Mailgun believes better sending practices make the inbox (and dare we say the world) a better place. Who wouldn't want to check their email to find it is free of spam and full of relevant messages they truly want to read?

We're not there yet. But in 2024, we made some progress. New sender requirements from Google and Yahoo nudged many organizations in the right direction. The truth is, you don't have to wait for mailbox providers to force you to make changes. There are many things you can do to enhance your email program and improve email deliverability.

Our research suggests a significant problem in the email community is a lack of understanding about deliverability. But you may not guess that if you asked senders. The survey found plenty of confidence around deliverability knowledge and the ability to implement supporting strategies – but is it a false confidence?

12%

are very confident in their deliverability knowledge.

35%

are **somewhat confident** in their deliverability knowledge..

17%

are **somewhat unconfident** in their deliverability knowledge.

6%

are **very unconfident** in their deliverability knowledge.

The remaining **30% took a neutral stance on their knowledge of deliverability** and abilities to improve inbox placement. In other words, they weren't sure how to answer.

While we did see some improvements from our inaugural survey (State of email deliverability 2023), there is still a lot of uncertainty around technical issues like infrastructure and authentication.

Likewise, plenty of senders who feel confident about deliverability were unable to correctly define one of the most fundamental email deliverability metrics – the delivery rate.

It's no shock that **avoiding spam was considered the biggest deliverability challenge** in both 2023 and the latest report. A missed opportunity, however, is that so few senders are taking the most effective step towards gaining clear visibility into inbox placement.

Only 13% of senders in our survey use inbox placement testing to find out where emails are likely to end up. But the reporting this seed testing provides is the most effective way to determine an inbox placement rate and make adjustments that improve email deliverability.

Improving email deliverability in the years to come will require in-depth knowledge, powerful tools, and expert partners who have your back.

“Mailbox providers are motivated to create a better, safer inbox experience for their users, but any organization that relies on email communication should want the exact same thing. How many brands can you name that don’t use email as a key part of their communication strategy?

From authentication to list management to improving email engagement, doing what’s best for email users leads to better deliverability and a higher return on your investment into an indispensable channel.”

Kate Nowrouzi
VP of Deliverability and Product Strategy
Sinch

CHAPTER 7

Looking ahead: The EAA and future-proofing your deliverability

In the past, or rather in the beginning, deliverability was mostly about infrastructure. If your IP was warm and your reputation was decent, and you had basic SPF and DKIM you were fine. But the definition of deliverability is evolving. Authentication, compliance, and now accessibility all factor in, and user experience is shaping the standard for sending.

Our survey and the data in this report shows the inbox has become more selective, more regulated, and more focused on recipient experience. And the trend is only going to continue. As of June 28, 2025 the European Accessibility Act taking effect, adding in another layer of expectation for senders.

However, the truth is still the truth, if you're a good sender, creating good emails, and caring about your perceived trust and sender reputation – you're going to be just fine.

Compliance is not a one-time thing

First it was Yahoogle. Then Microsoft. Now accessibility has taken the headlines.

With the European Accessibility Act taking effect on June 28, 2025, brands sending email to EU consumers will be legally required to meet digital accessibility standards. That means the structure, content, and design of your email must be usable for people with disabilities. In other words, it's time for email for all.

This act isn't just a checkbox for devs to deal with. Accessibility is a deliverability issue. It is a usability issue. And it is a brand trust issue.

Accessibility applies to more than just screen readers

Accessibility in email often gets reduced to alt text and ARIA labels, but it goes deeper than that. Think visual hierarchy, color contrast, meaningful headings, and assistive tech compatibility.

> “Most of the accessibility issues in email are fixable with structure, hierarchy, and color contrast. That means your email templates matter. So do your fallback experiences. And your design system, your copy, and your development tools all need to support a more inclusive experience.”

Megan Boshuyzen
Sr. Email Developer, Sinch Mailgun and Mailjet

According to the World Health Organization, we have an estimated **1.3 billion people who have disabilities**, and that is about 16% of the world population. 4.6 billion of those users use emails, so around **736 million email users have disabilities**.

And it’s not just a user experience stat. If you’re not thinking about accessibility, you’re leaving roughly **59 million dollars on the table.**

Email that works for more people performs better

Accessibility is not only the right thing to do, it’s also good sending. Accessible emails are easier to read, faster to understand, and build trust with your audience.

These emails tend to load faster, be more scannable, and improve engagement metrics like opens, clicks, and unsubscribes. And since mailbox providers use recipient behavior to decide if you belong in the inbox, accessible design indirectly boosts your deliverability.

And therein lies the hidden benefit of getting ahead of EAA. You are not just complying. You are optimizing.

Future ready means people ready

Deliverability used to be all about reputation and infrastructure. Now it’s also responsibility to email subscribers and making the inbox a better, safer place.

Mailbox providers are raising the bar, first Yahoogle and now Microsoft. Users are expecting more and governments are demanding accessibility be factored in. Legislation is catching up. But the senders who get this right will keep their spots in recipient inboxes as standards continue to evolve.

> “Accessibility isn’t about checking a box, it’s about making your email readable and functional for everyone. That’s just good sending.”

Megan Boshuyzen
Sr. Email Developer, Sinch Mailgun and Mailjet

What comes next for email

We’re seeing a shift that’s more than just technical updates or policy changes. The future is looking like a long-term movement toward user-first email. That means putting transparency, usability, and identity at the center of every message.

Authentication, Compliance, Accessibility, these are the three foundational pillars. Senders who invest in that foundation now will not only stay ahead of changes like the EAA; they’ll be better positioned for whatever inbox expectations come next.

The future of email is not about finding new tricks. It’s about getting the basics right and keeping them right.

MAILGUN INSPECT

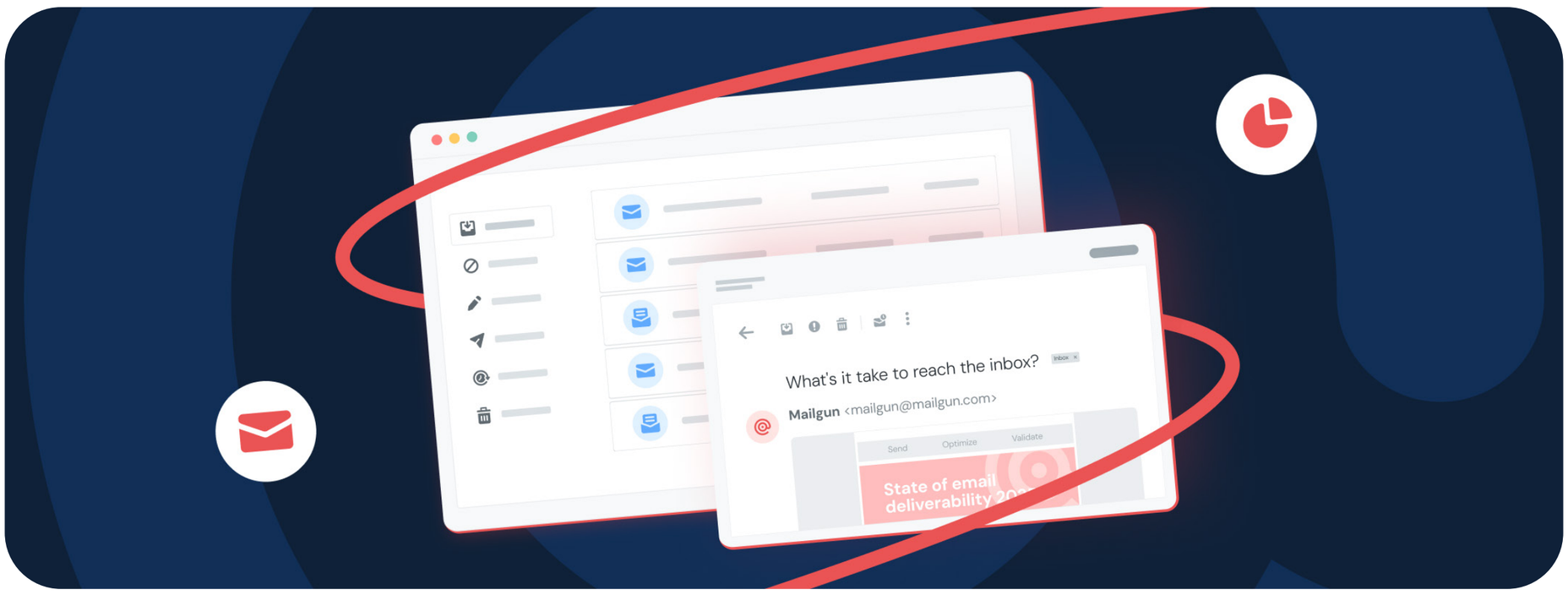
How will you know if your emails are accessible?

What if you could catch accessibility issues, broken links, and inbox render problems before you ever hit send?

With automated testing for accessibility, subject lines, CTA performance, and client rendering across 100+ environments, Inspect is built for email senders. Get pre-send clarity on what works, what breaks, and what’s holding your emails back from the inbox.

This testing suite is available to all Mailgun customers and free to try in our open pilot program. Contact the Sinch Mailgun team to get started.

Find Out More



CHAPTER 8

About this survey

During July of 2024, Sinch Mailgun conducted a global survey of email senders. Respondents included Sinch Mailgun users as well as users from sister brands Sinch Mailjet and Sinch Email on Acid. The survey collected data and insights concerning the email deliverability knowledge and practices of senders around the world.

More than 1,100 participants completed the survey. Respondents were invited to participate via email messages and in-app notifications. They were also incentivized by the chance to win a $100 Amazon gift card, which was awarded to one random participant.

See further information below for a breakdown of respondent demographics. Due to rounding, some survey results may exceed or fall short of 100% by a difference of 0.1%.

Respondent demographics

Regions	Industries
United States – 27.5%	Information Technology (IT) – 12.7%
France – 23.0%	Software as a Service (SaaS) – 11.3%
Germany – 6.1%	Non-Profit – 8.5%
United Kingdom 5.0%	Marketing/Public Relations – 7.1%
Canada – 3.1%	Professional Services – 6.6%
Spain – 2.9%	Retail/ecommerce – 5.6%
India – 2.5%	Education – 4.6%
All other regions – 29.9%	Entertainment/Recreation – 4.2%
	All other industries – 39.4%

Monthly email send volumes	Job title/role
More than 1 million emails – 11.4%	Small business owner – 15.6%
100,000 to 1 million emails – 12.8%	Software developer – 14.4%
50,000 to 100,000 emails – 13.4%	IT professional – 14.1%
Fewer than 50,000 emails – 62.5%	Marketing leadership – 9.8%
	Email marketer – 8.4%
	C-suite executive – 5.8%
	Director/VP of product – 5.4%
	Email deliverability specialist – 5.2%
	Product management – 5.1%
	Lifecycle marketing manager – 2.2%
	Other roles – 13.5%

Business size	Users
10 or fewer employees – 52.3%	Sinch Mailgun – 39.1%
11 to 50 employees – 21.8%	Sinch Mailjet – 47.3%
51 to 500 employees – 17.3%	Sinch Email on Acid – 13.6%
501 to 1000 employees – 3.2%	
1,001 to 5,000 employees – 2.7%	
More than 5,000 employees – 2.6%	

Business type
B2B – 37.6%
B2C – 29.4%
Both B2B and B2C – 33.0%

SINCH Mailgun

Sinch Mailgun, part of Sinch's Customer Communications Cloud, powers 450B+ emails at scale across the globe annually. We recognize email is one of the core drivers of a brand's return on investment in digital marketing; our unified, scalable, and customizable platform supports the overarching lifecycle management of email, with security, compliance, and data privacy at the forefront. We align with all major global standards and regulations such as GDPR, SOC I & II, HIPAA, and ISO 27001.

Sinch Mailgun's industry-leading product offerings include:

- **Mailgun Send:** A platform to send, receive, automate, and track emails at any scale.
- **Mailgun Optimize:** A suite of email deliverability tools to improve inbox placement and connect with more people.
- **Mailgun Validate:** An enterprise solution for keeping email lists clean and sender reputation strong.

sinch

Sinch is pioneering the way the world communicates. More than 150,000 businesses – including many of the world's largest tech companies – rely on Sinch's Customer Communications Cloud to improve customer experiences through mobile messaging, voice, and email.

Sinch has been profitable and fast-growing since it was founded in 2008. It is headquartered in Stockholm, Sweden, with shares traded at NASDAQ Stockholm: XSTO: SINCH. Learn more at **sinch.com.**