



# Welcome

**Our webinar will start soon**



---

# Data Interpretation & Industry Updates



# Discussion Points for Today



## Data interpretation

Interpreting the data in the  
Sendmarc Client Portal

Data insights tailored to  
different personas



## Partner Toolkit

Black Friday and Cyber  
Monday Partner Toolkit



## Industry news

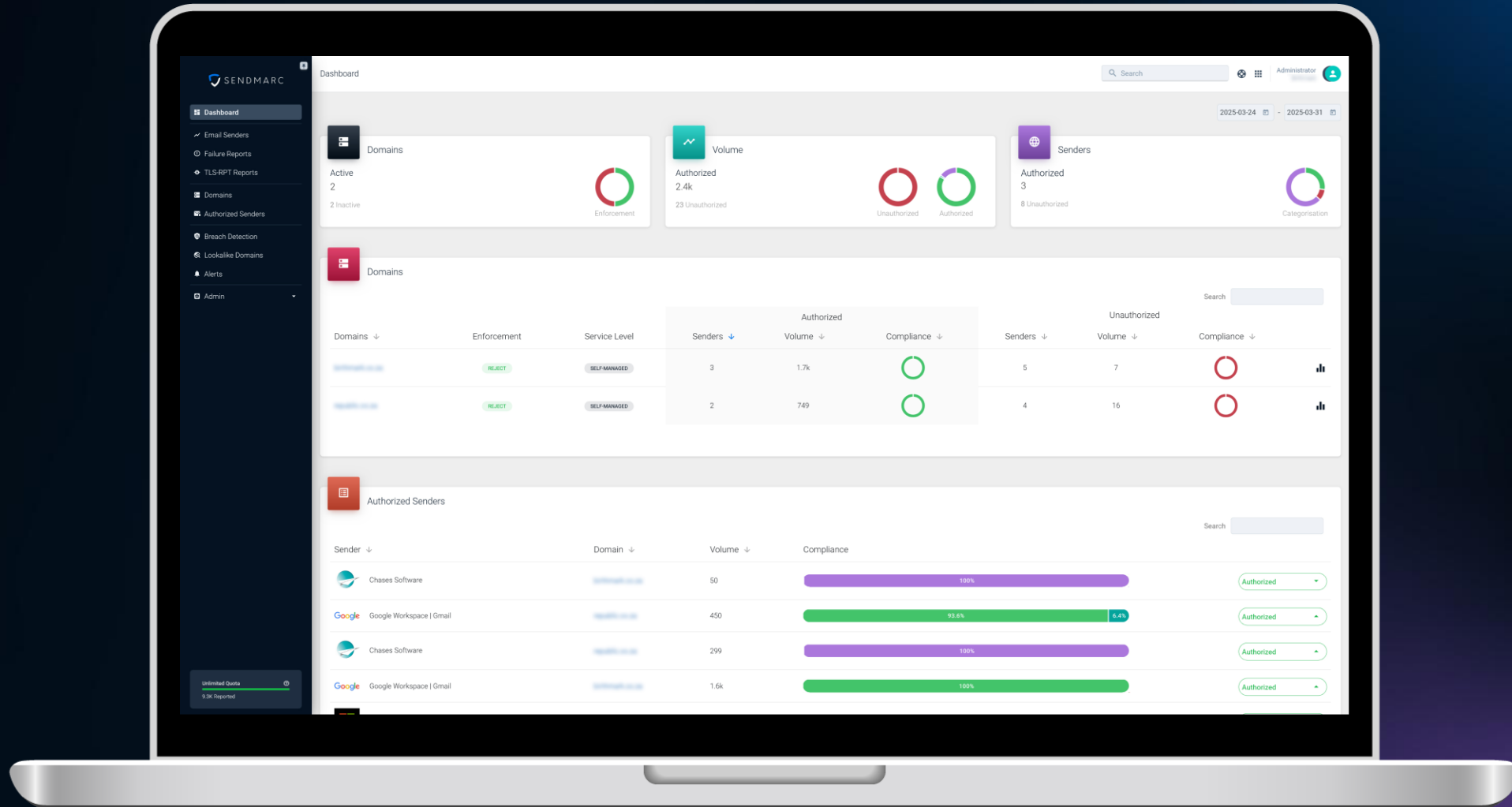
Looking at  
DMARCbis

The background is a complex digital visualization. It features a large, glowing blue shield shape in the center-right, which is filled with a network of red and blue lines and nodes, resembling a data graph or a secure digital space. The shield is set against a dark blue background with swirling patterns of light and data points. On the left side, there is a solid blue rectangular block. The overall aesthetic is high-tech and futuristic, with a color palette dominated by blues, reds, and purples.

# Data Interpretation

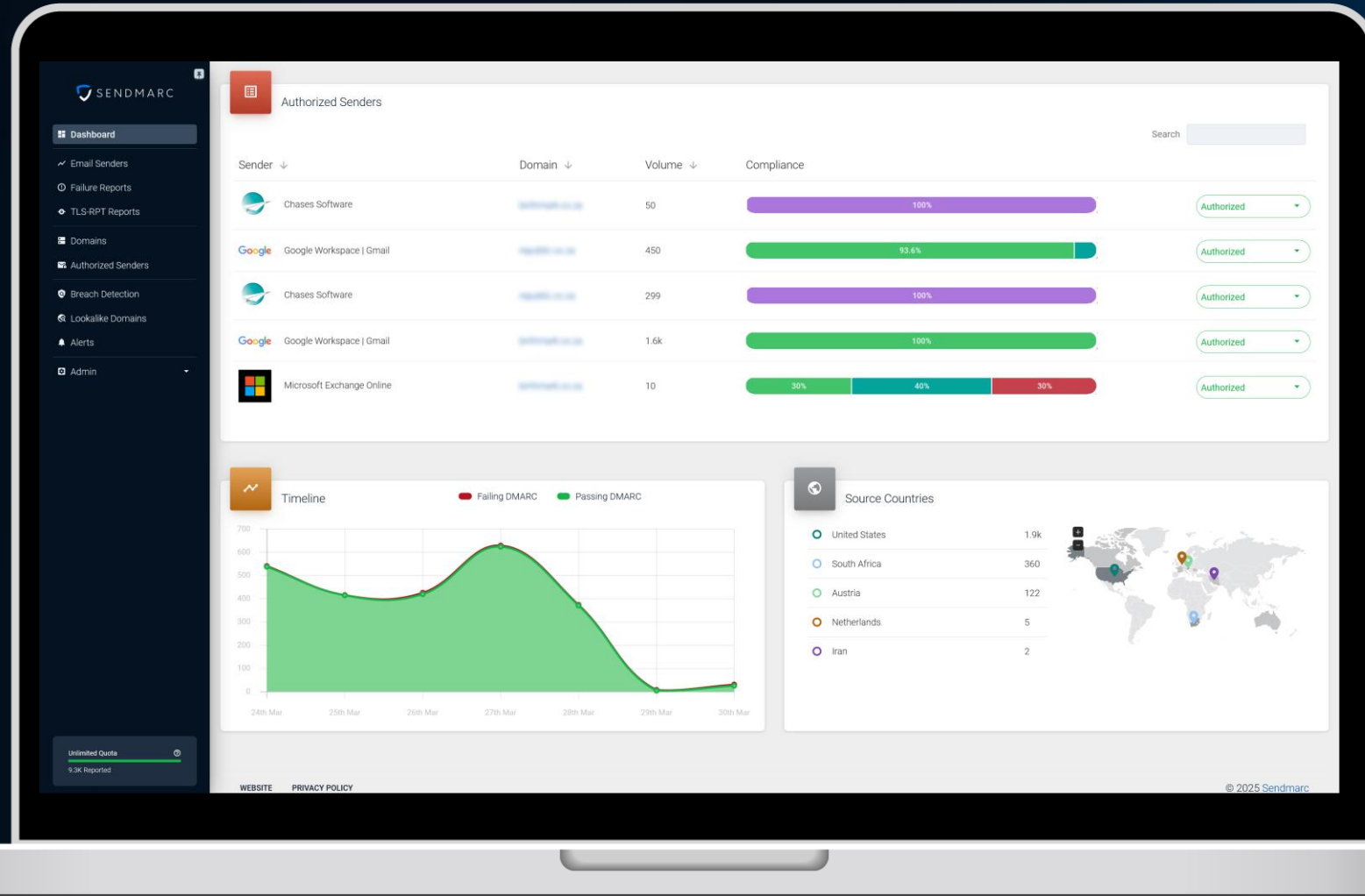
# Dashboard View

The Dashboard view in the [Sendmarc Client Portal](#) provides an overview of statistics, sources, senders, and email volumes relevant to all domains in the account over a certain date range.



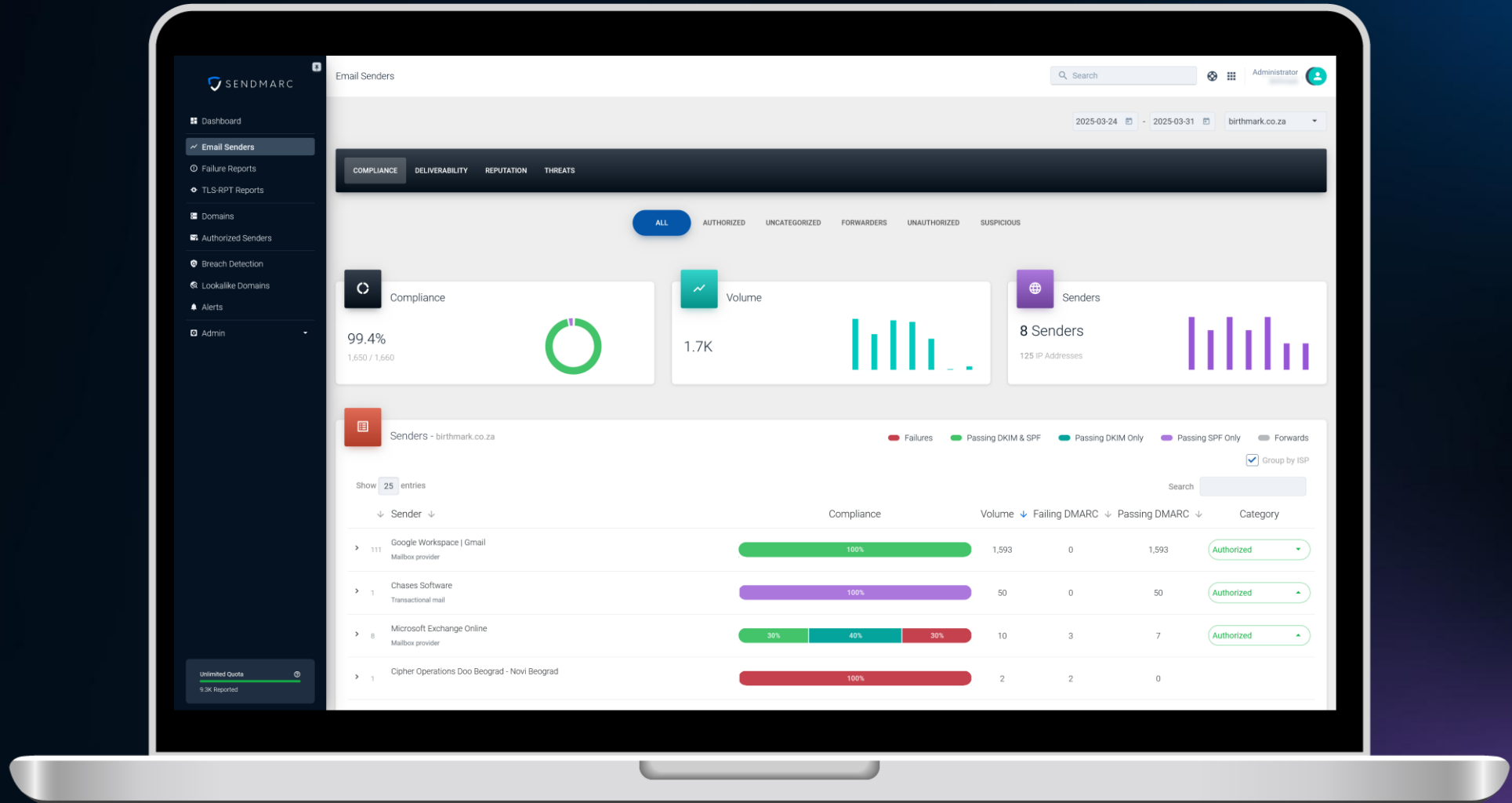
# Dashboard View

The Dashboard view in the [Sendmarc Client Portal](#) provides an overview of statistics, sources, senders, and email volumes relevant to all domains in the account over a certain date range.



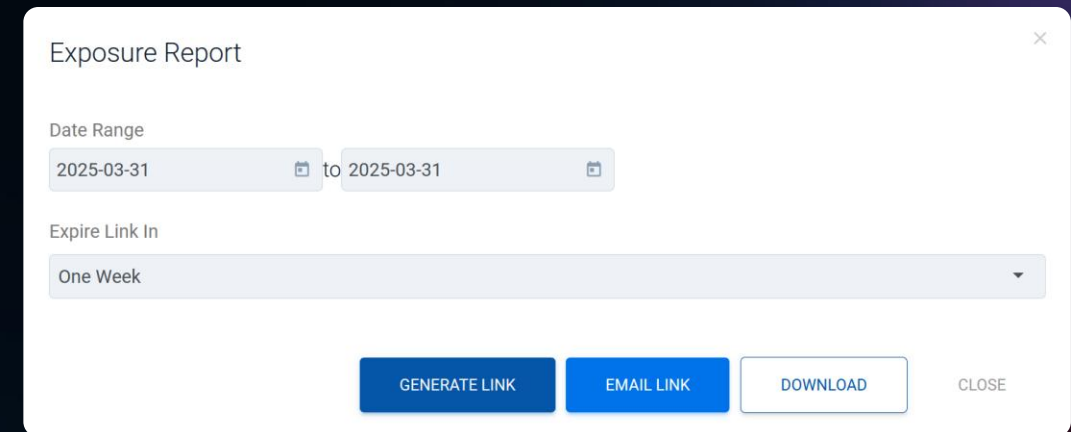
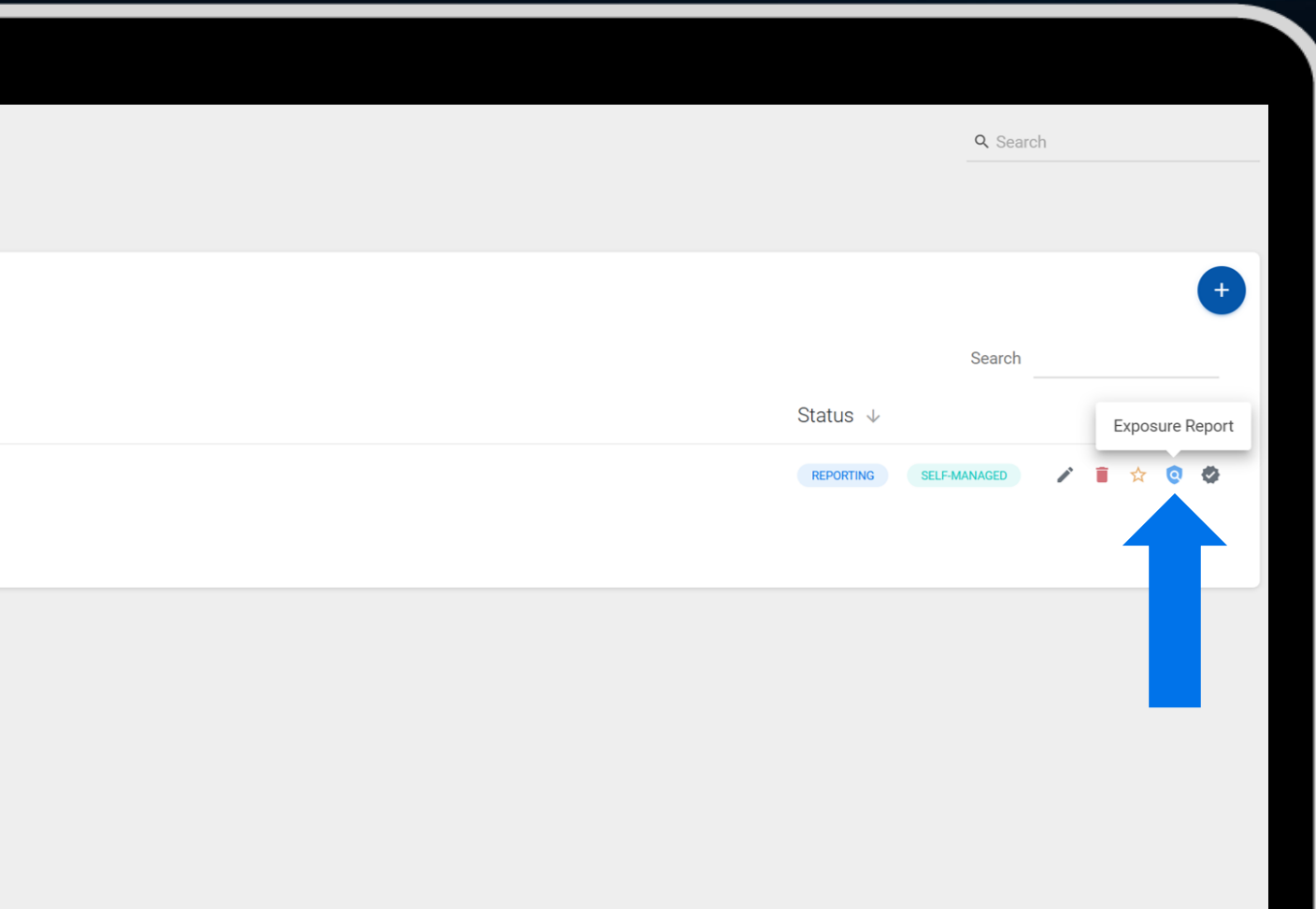
# Email Senders

The Email Senders view provides insights into the compliance levels, deliverability statistics, IP reputation, and threat sources for a specific verified domain in an account.



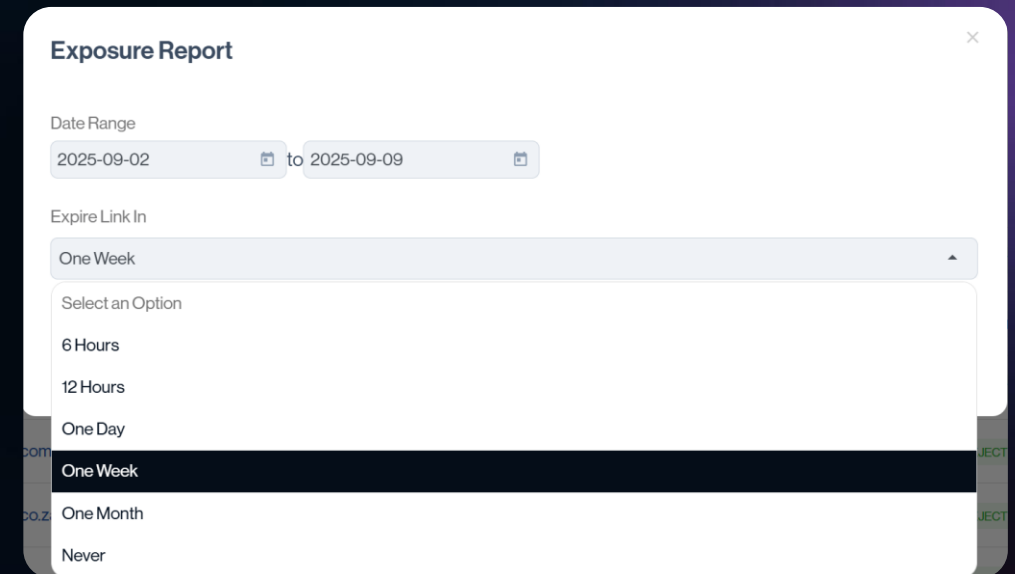
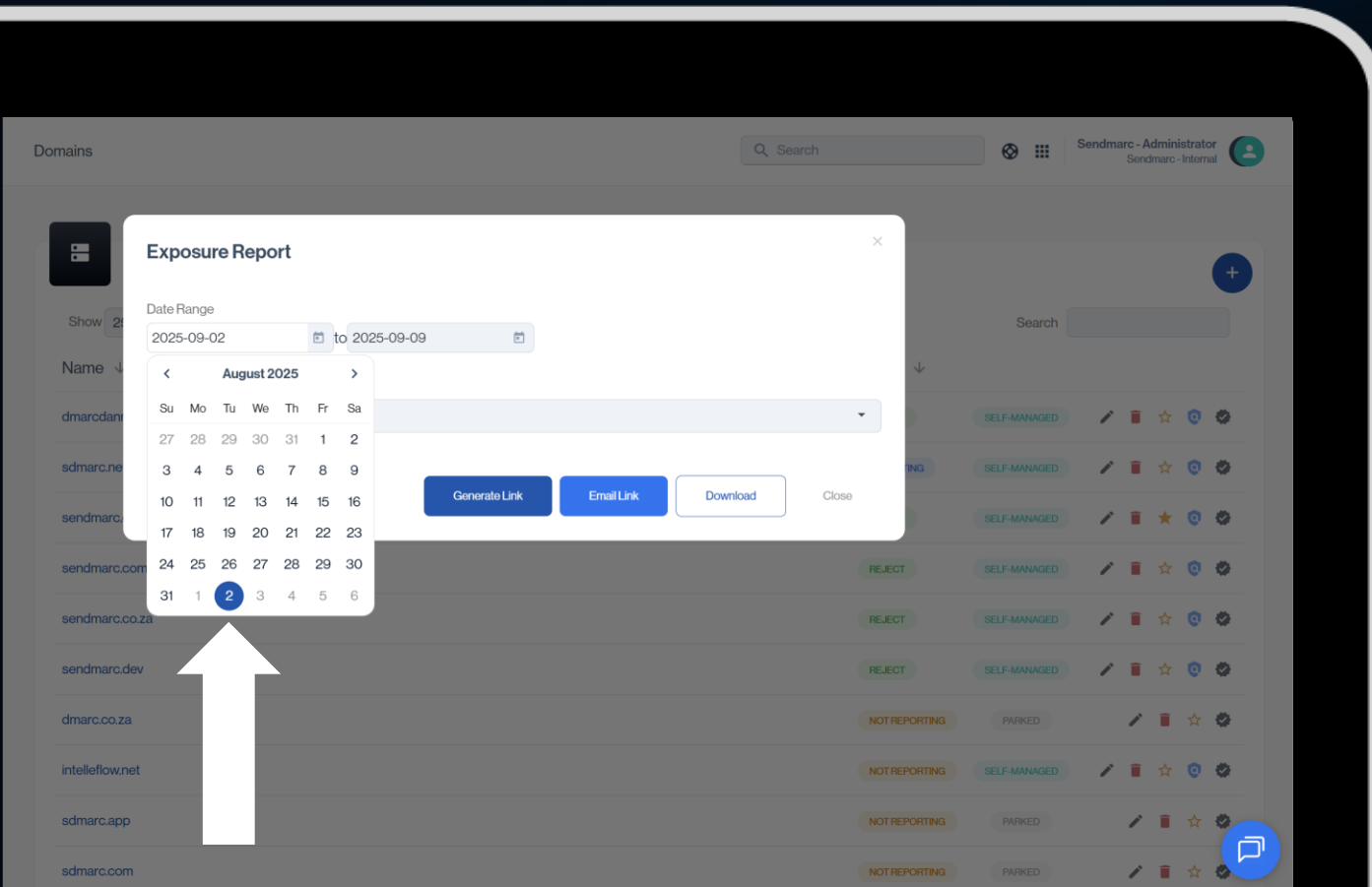
# Generating an Exposure Report

To get or share an exposure report, you can generate a shareable link, email the download link to a specified address, or download the report as a PDF. First, select the date range you'd like the report to cover, then click the relevant button.



# Generating an Exposure Report

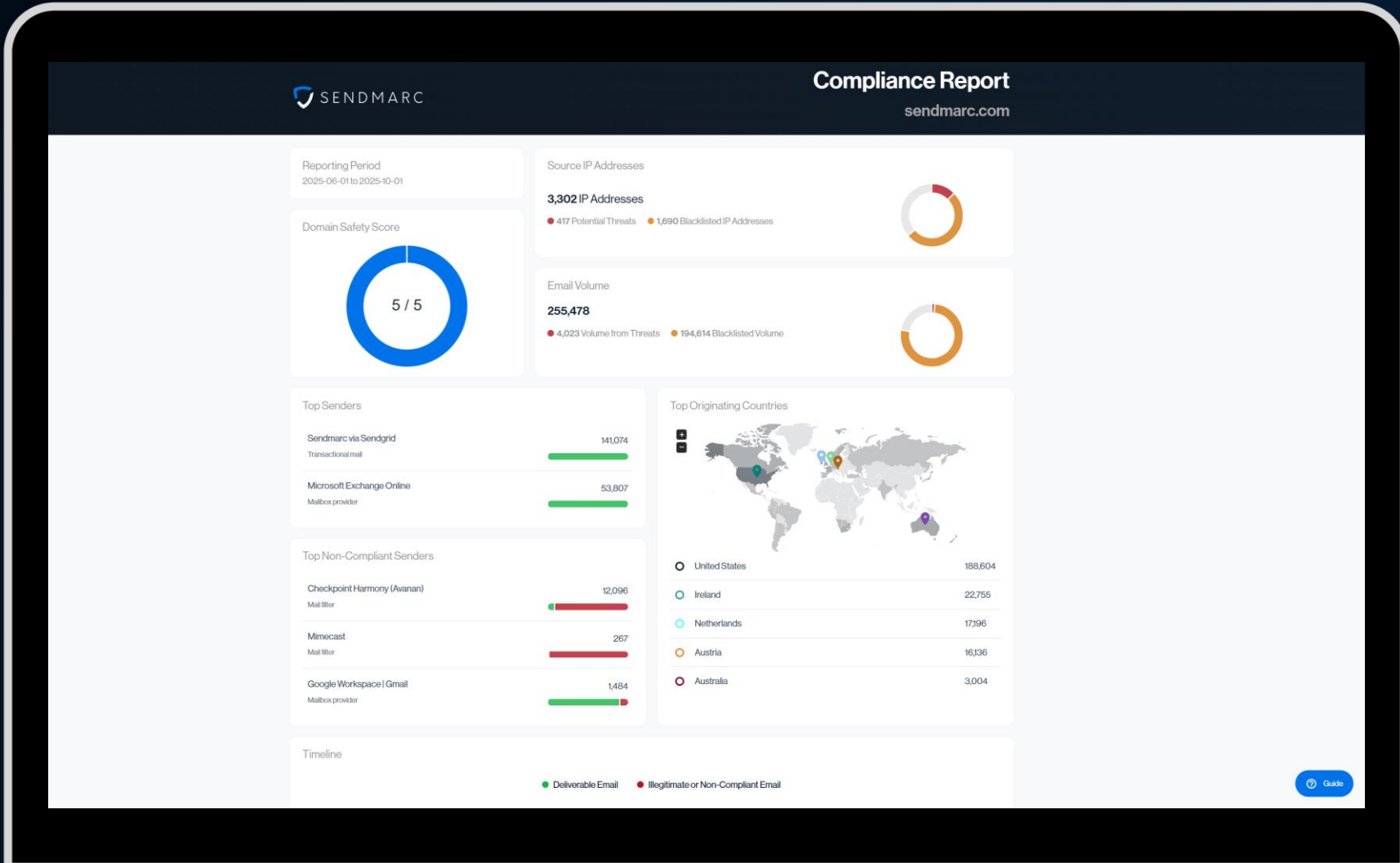
When generating an exposure report, your organization can either download it or send it to an email address



# Complete a Live Demo

<https://portal.sendmarc.com/guarded/1f1c026c-f951-41c4-9692-13b8c3fa9089/42f0bf8542dd7fe2369ae57c4cfe3503fa280fbcac4a1cd7a6425d9a372674b0/resource/10995beb-dbc2-49fc-b3d3-61175e86e3b5/domain/exposure-report>

# Sendmarc Exposure Report



Navigate through an exposure report using the Guide function



Welcome to the Exposure Report for sendmarc.com

This tutorial will walk you through interpreting the report.

Skip Next

# Understanding an Exposure Report

## Domain safety score

The screenshot shows the SendMARC Compliance Report interface. At the top left is the SendMARC logo. The title "Compliance Report" and the domain "sendmarc.com" are at the top right. The "Reporting Period" is "2025-06-01 to 2025-10-01". A "Domain Safety Score" of 5/5 is displayed in a large blue circle. A tooltip explains: "This is your Domain Safety Score. It's an overall view of how protected your organisation is." Other metrics include "Source IP Addresses: 3,302 IP Addresses" (with 417 Potential Threats and 1,690 Blacklisted) and "Email Volume: 255,478" (with 4,023 Volume from Threats and 194,614 Bounces). Navigation buttons "Skip", "Previous", and "Next" are visible.

## Sending sources

The screenshot shows the "Sending sources" section of the SendMARC Compliance Report. It includes a legend: "Each sender listed here sends mail from sendmarc.com. Mail sent in a compliant manner is green. Non-compliant mail is red. A complete list of senders can be seen inside Sendmarc." Below this are two lists of senders with their respective counts and compliance status, shown as horizontal bars.

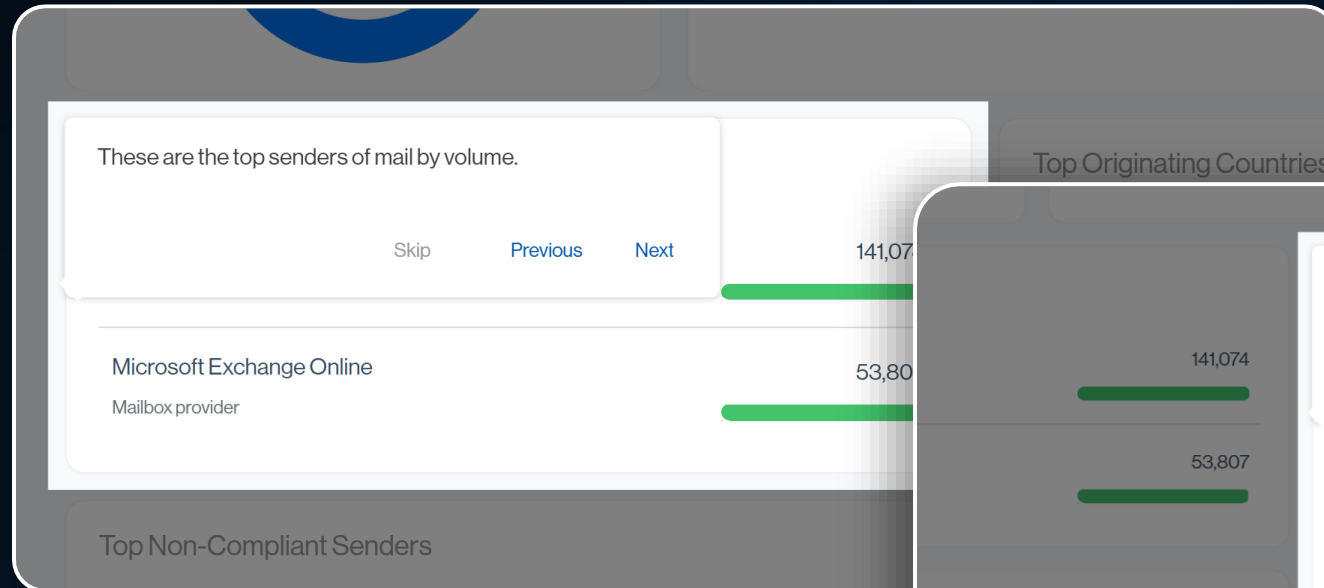
Sender	Count	Compliance Status
Microsoft Exchange Online	141,074	Compliant (Green)
Mailbox provider	53,807	Compliant (Green)
Checkpoint Harmony (Avanan)	12,096	Non-compliant (Red)
Mail filter	267	Non-compliant (Red)
Mimecast	267	Non-compliant (Red)
Mail filter	1,484	Non-compliant (Red)
Google Workspace   Gmail	1,484	Compliant (Green)
Mailbox provider	1,484	Compliant (Green)

On the right, "Top Originating Countries" are listed with a world map showing the United States as the primary source.

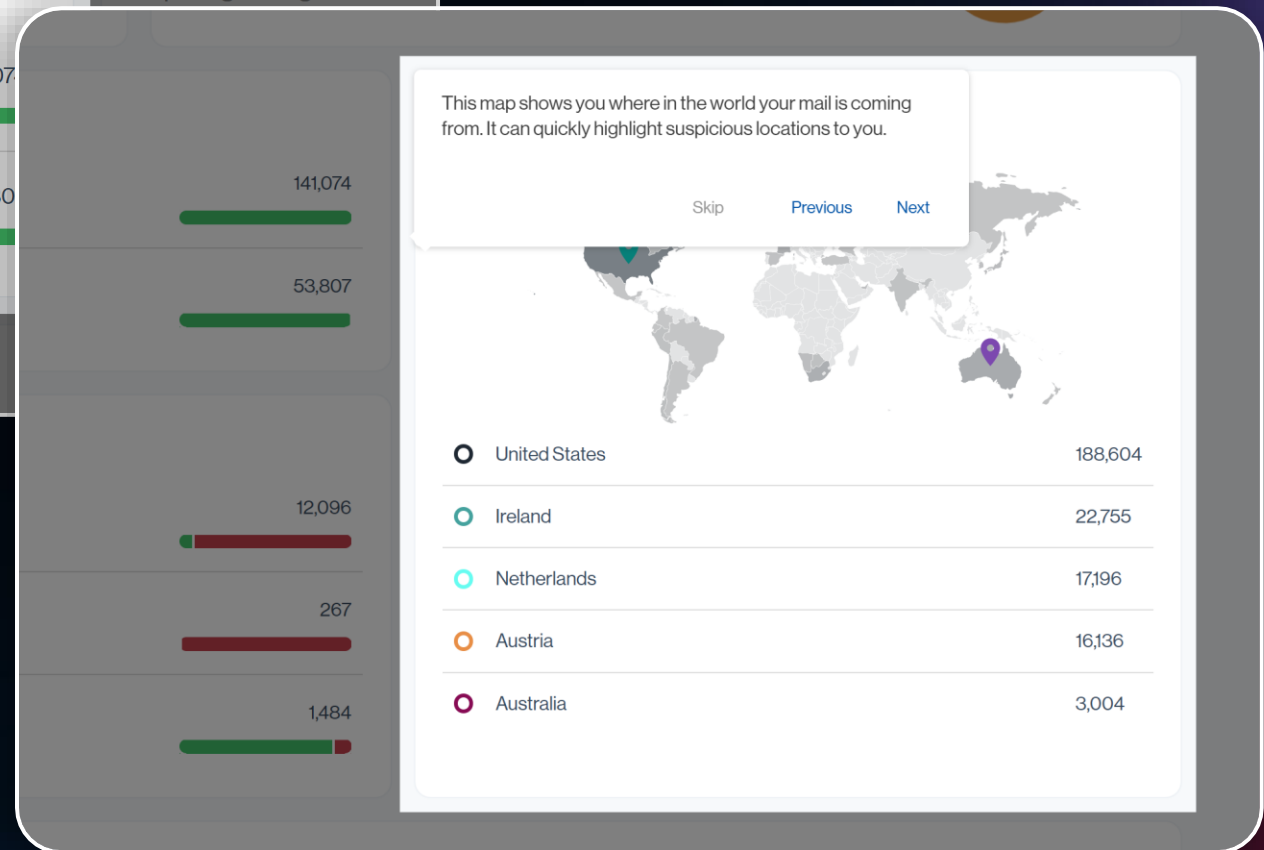
- United States
- Ireland
- Netherlands
- Austria
- Australia

# Understanding an Exposure Report

## Sending sources volume



## Source countries





# Understanding an Exposure Report

## Exposure

This section will highlight some areas where your organisation is open to risk.

Skip Previous Next

You may not receive reports on all volume

- You are not receiving failure reports making it harder to find senders abusing your domain
- Unauthorised sending servers may be allowed to send from your domain

## Recommendations

Lastly, this section will make some recommendations around next steps for your environment.

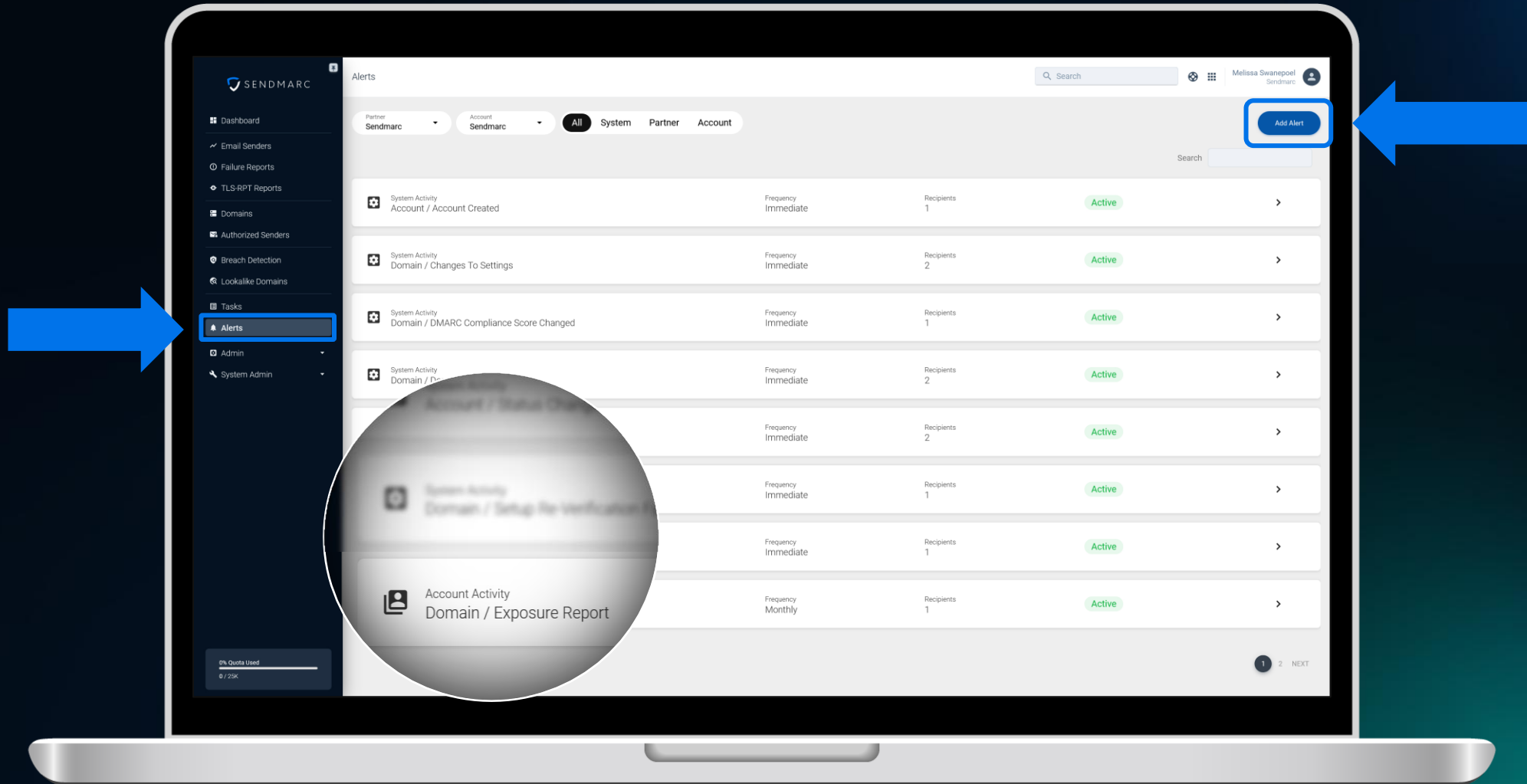
Skip Previous Next

- Add the Sendmarc failure report addresses to your DMARC record for in-depth error reporting
- Set your SPF record to hard fail when a sender is not authorised

© 2025 Sendmarc

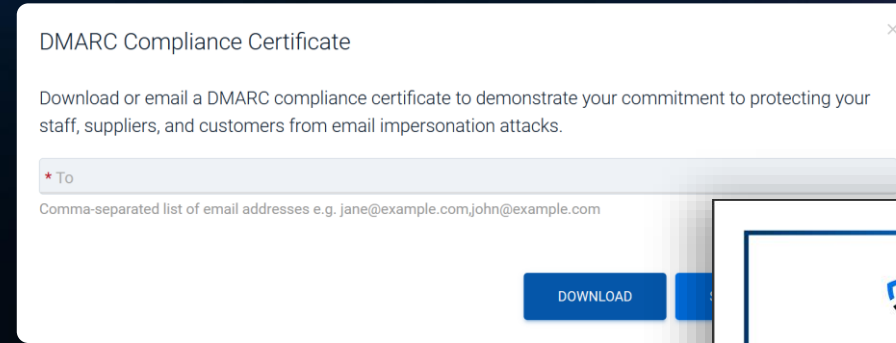
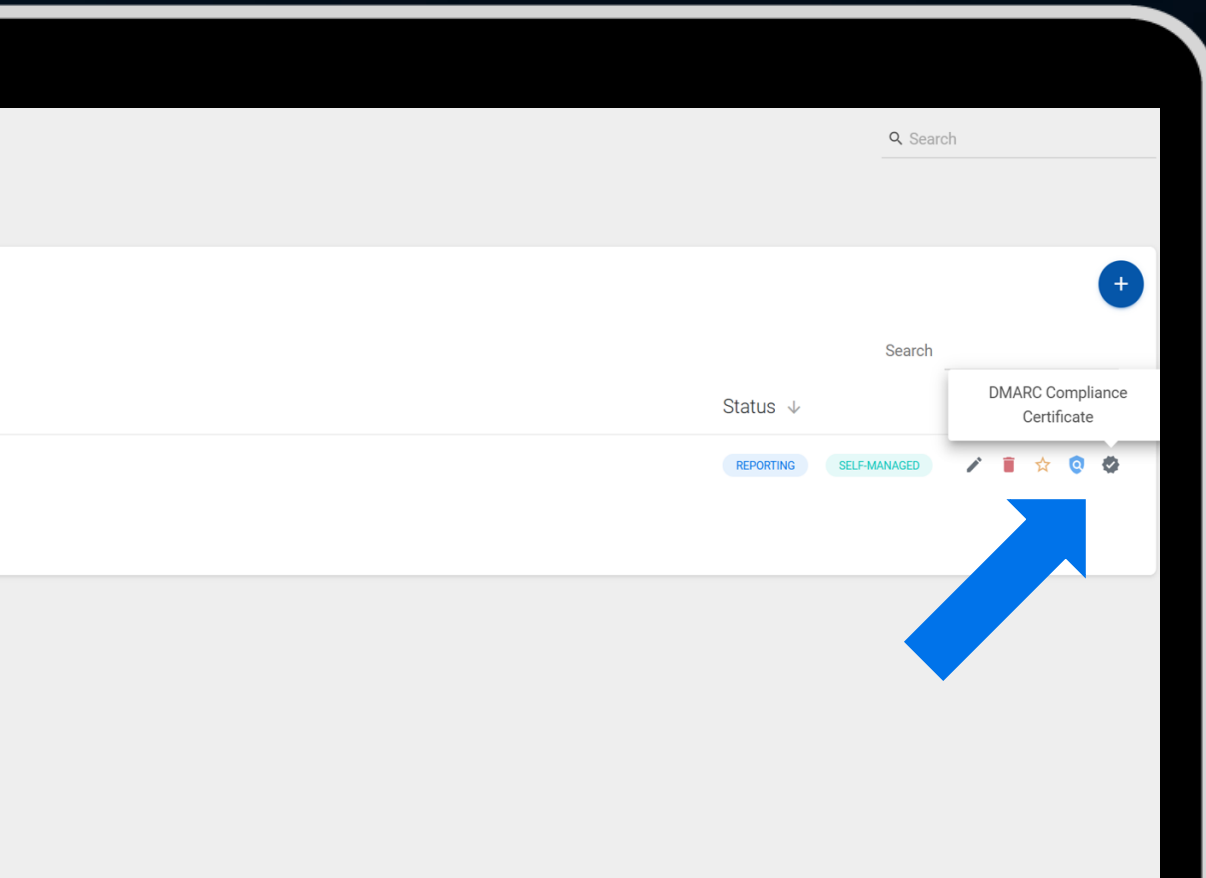
# Setting Up Alerts

Configure alerts to stay updated on changes in your business's partner and customer accounts – you can specify the alert frequency and recipients.



# Generating a Compliance Certificate

When generating a DMARC compliance certificate, your organization can either download it or send it to an email address.



# Security Leaders

## Who

The CTO of a medium-sized organization with a focus on cybersecurity. He's a technical whizz who manages the company's IT infrastructure.

## Goals

- Improve visibility and reporting
- Create confidence in policy enforcement
- Enhanced compliance regulation

## Top concerns

- Unauthorized senders
- Lookalike domains
- Deliverability

## Needs

- Access to real-time visibility into email domain activity
- Real-time threat monitoring
- Visibility into unauthorized use of domain

## The Sendmarc Solution

- Sendmarc Customer Platform
- Implementation support and process
- Reporting and monitoring

With real-time alerts and reporting, Charlie can take corrective actions and continuously improve the organization's email security, mitigating potential financial and reputational risks.

## Charlie | CTO



# Finance Leaders

## Who

The CFO of a medium to large-sized organization. He's responsible for managing the financial aspects of the company and ensuring cost-effectiveness in all departments.

## Goals

- Use a cost-effective, scalable solution
- Compliance and regulation
- Reduce costly cyberattacks
- Reduce legal and insurance costs

## Top concerns

- Cash-flow protection
- Business Email Compromise (BEC)
- Audit and compliance readiness

## Needs

- Simple pricing model
- Proactive risk management
- Enhanced customer experience and trust

## The Sendmarc solution

- Protects domains
- Flags unauthorized senders and lookalike domains
- Protects revenue and ensures only legitimate emails are delivered

## David | CFO



# Marketing Leaders

## Who

The CMO of a company, who is responsible for developing and executing marketing strategies to drive brand awareness and customer engagement. She understands the importance of maintaining a strong brand reputation and customer trust.

## Goals

- Boost brand awareness
- Grow ROI
- Ensure deliverability of emails

## Top concerns

- Brand integrity and trust
- Visibility of email performance
- Disruption to email campaigns

## The Sendmarc solution

An email authentication standard like Brand Indicators for Message Identification (BIMI), that allows Maya to display her organization's logo next to emails in recipient inboxes. DMARC and BIMI work together and provide benefits such as:

- Increased trust in the sender
- Improved email deliverability
- Reduced phishing and spoofing attacks
- Improved brand awareness and recognition

Emails authenticated with BIMI have a higher chance of going to the recipient's inbox and not their Junk or Spam folder.

## Maya | CMO





# Black Friday and Cyber Monday Toolkit

# Get Ready for Black Friday and Cyber Monday

In preparation for Black Friday and Cyber Monday, please download your Partner Toolkit from the [Partner Portal](#).

## Assets included:



Email template



Email banner



**The increase in online shopping during the Q4 holiday season brings more email scams.**

**Your toolkit includes ready-to-use assets to spark timely conversations and drive free outbound email audit requests.**



# Industry News



# DMARCbis is Coming:

## The next generation of email authentication (DMARC 2.0)

### What is DMARCbis?

DMARCbis, also known as DMARC 2.0, is a proposed DMARC update designed to keep pace with modern email threats. It introduces important updates designed to make email authentication more reliable and easier to implement.

### Key updates

DMARCbis brings key updates to make email authentication stronger, simpler, and more effective against modern threats.



# What is changing in DMARCBis?

Below are the changes security teams and domain owners need to know:

## DNS Tree Walk

Replaces the Public Suffix List (PSL) with a DNS-native method for determining organizational boundaries.

## New tags

New policy tags have been introduced to give businesses finer control and help define which domains are public suffix domains and which are organizational domains.

## Removed tags

Pct (percentage-based enforcement), rf (report format), and ri (report interval) are being removed to simplify DMARC records for easier management with fewer inconsistencies.

## Enhanced reporting

The specification is being reorganized, with clearer definitions, better examples, and better guidance for both senders (domain owners) and receivers (mail services) about how to correctly participate.

# Why this matters

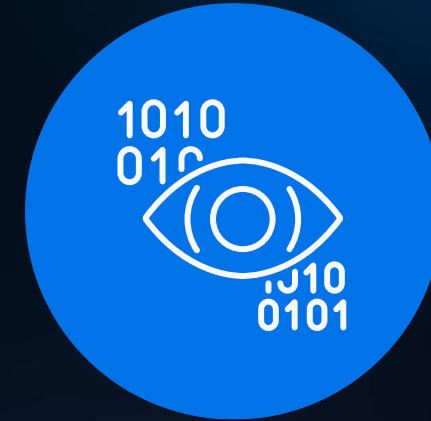
DMARCBis introduces key improvements that will benefit your business by:



Providing improved protection for complex domain setups



Reducing errors that cause phishing or block valid emails



Providing clearer reports to help security teams act faster and with confidence

# Webinars for the Year

Access our previous webinars under the 'Resources' section on the [Partner Portal](#)

The rise of DMARC and other industry updates

**February**



Sendmarc Client Portal and industry updates

**April**



Product spotlight and industry updates

**June**



Pitch like a pro: part two and industry updates

**August**



Sendmarc sales masterclass

**October**



**March**

Uncover DMARC updates and sales tips



**May**

Sendmarc Partner Portal: key updates and insights



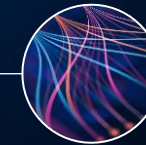
**July**

Pitch like a pro: part one and industry updates



**September**

Deal registration and cybersecurity month





**We would love to get your input!**

What are some webinar topics you'd like us to cover next year?

# Win a \$100 Voucher

Gain free access to our Certified Sendmarc Salesperson Courses!

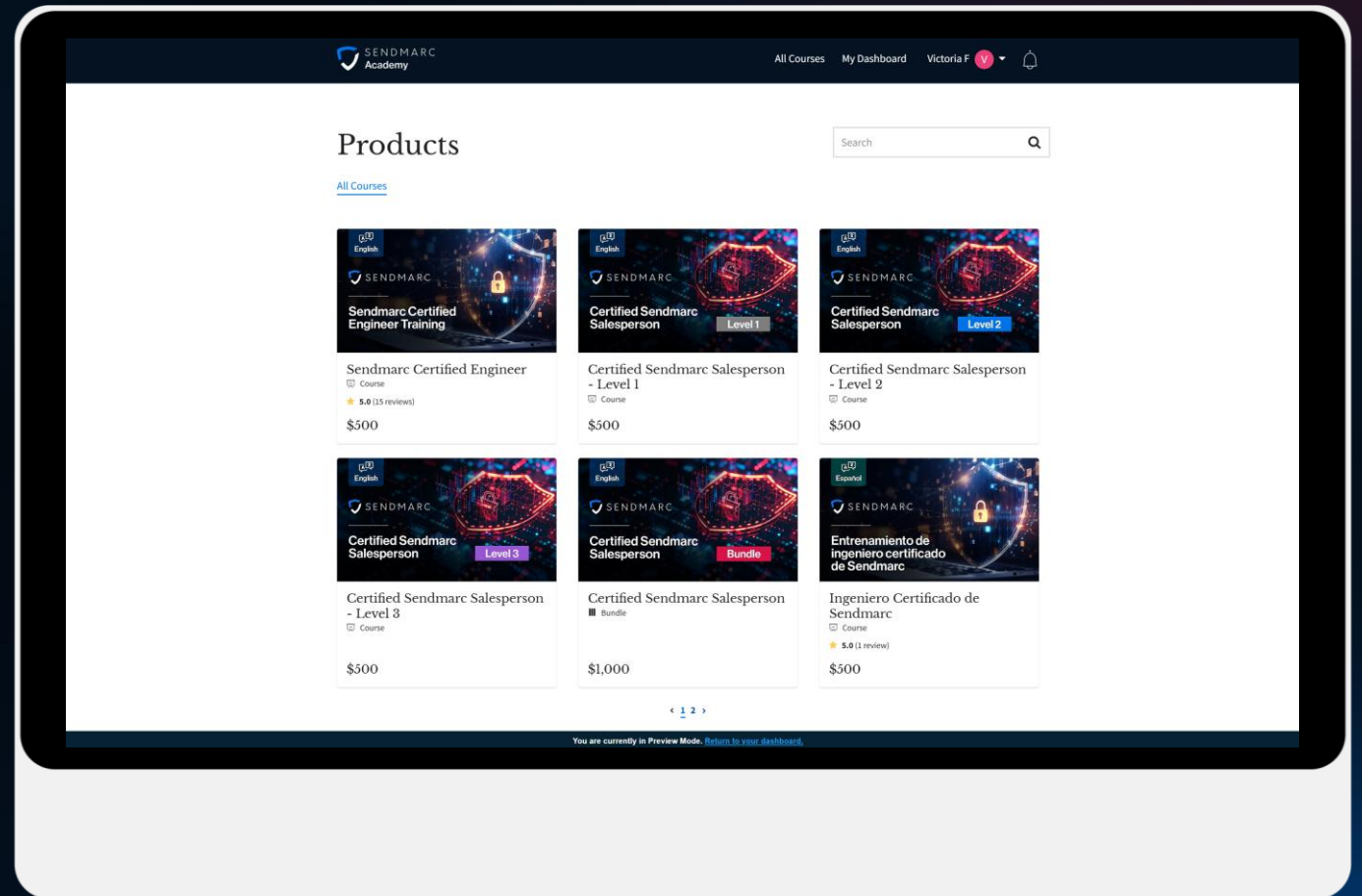


Enter our monthly draw for a chance to win a \$100 voucher\*

\*Or region equivalent

- 1 Enrol in one of our courses
- 2 Complete the training & quizzes
- 3 Obtain your certification
- 4 Post it to LinkedIn & tag us

[academy.sendmarc.com](https://academy.sendmarc.com)





# Thank You

[www.sendmarc.com](http://www.sendmarc.com) | [channel@sendmarc.com](mailto:channel@sendmarc.com)