Remi IT
SOLUTIONS

DMARC Management

A 2024 Email Security Landscape Report for Massachusetts and Rhode Island

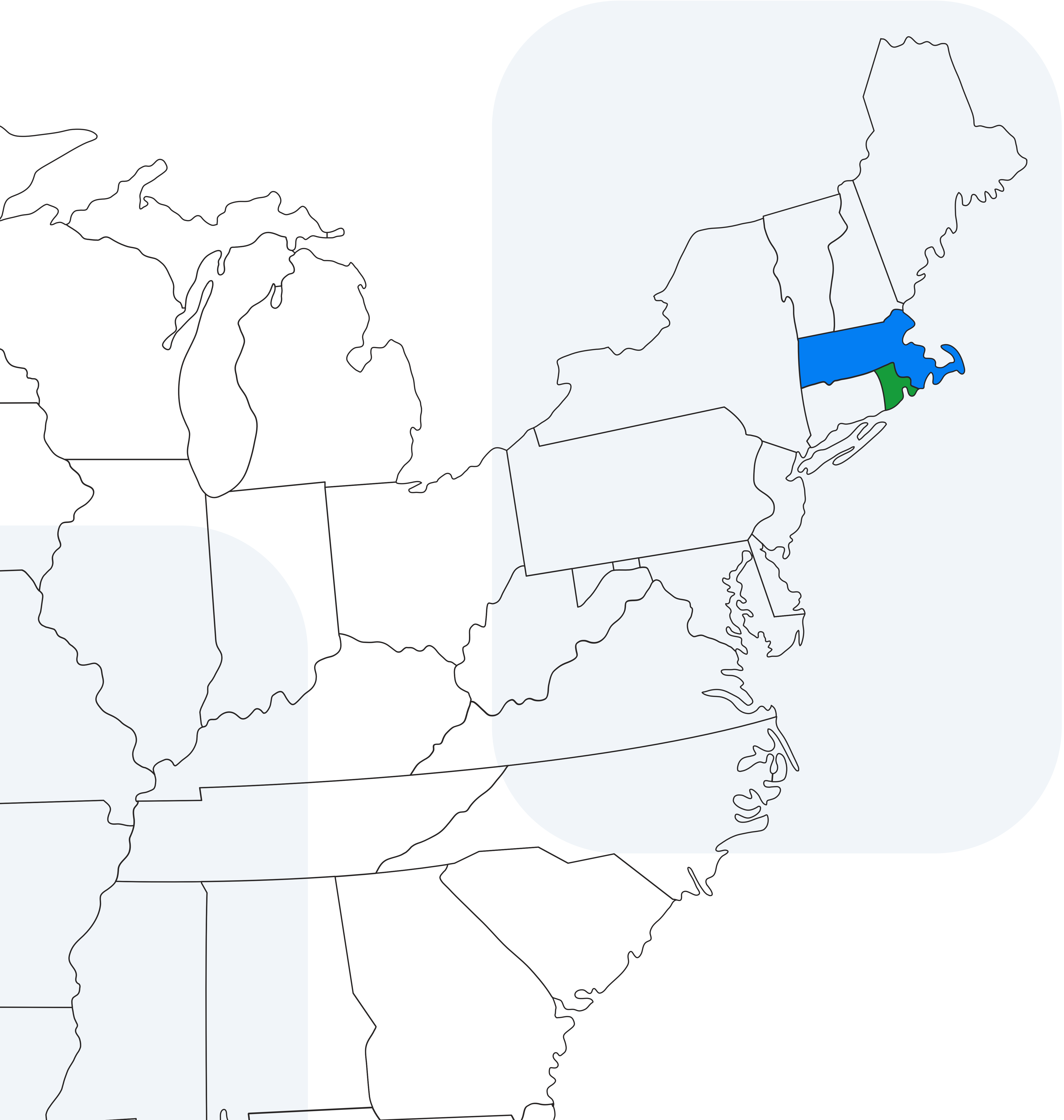
Introduction

As cyber threats continue to evolve, particularly in the form of email spoofing and phishing, the implementation of robust email security policies is critical for enhancing overall security and preserving the integrity of business communications. This report examines the DMARC (Domain-based Message Authentication, Reporting, and Conformance) policies of 400 major organizations across Massachusetts and Rhode Island.

By evaluating the adoption and effectiveness of DMARC policies, this report provides valuable insights into the overall state of digital security within some of the largest and most influential organizations in the region. This report looks at the current landscape of email authentication practices among leading corporations, higher education institutions, healthcare organizations, and government entities in these states – identifying trends, compliance levels, and potential vulnerabilities in their approach to thwarting email-based security threats.

Introduced in 2012, the DMARC standard facilitates the automatic detection and elimination of emails that impersonate sender domains, serving as a vital method to thwart phishing and spoofing attacks.

Remi IT Solutions compiled a list of 400 of some of the largest organizations with offices in Massachusetts and Rhode Island by estimated annual revenue. Two hundred organizations' domains were examined from each state. This report will look at the email security policies for the region, as well as by state. Understanding the email security landscape for some of the largest organizations in the region helps to get a better understanding of the improvements needed for all businesses operating in Massachusetts and Rhode Island. No matter the size, every organization should and can be equipped with strong email security policies.



Highlights

Despite their vast resources, many of the largest organizations in Massachusetts and Rhode Island have email vulnerabilities which can be easily identified by cybercriminals.

MASSACHUSETTS

61%

of Massachusetts organizations have weak DMARC policies.

RHODE ISLAND

76.5%

of Rhode Island organizations have weak DMARC policies.

Almost all organizations in Massachusetts and Rhode Island lack adoption of the newest email security policies.

An enormous opportunity exists for organizations of all sizes to strengthen their email security policies in 2024.

What is DMARC?

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is an email validation system designed to protect email domains from unauthorized use, a practice commonly known as email spoofing. DMARC builds upon two key email authentication methods: Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM). SPF validates emails by verifying sender IP addresses, while DKIM ensures the content integrity of the email through cryptographic authentication.

Strong DMARC Policies Make Stronger Organizations

To implement a strong DMARC policy, a business should start with a policy of `none` to monitor and collect data on email flows, then move to `quarantine` to allow suspicious emails to be held aside by receiving servers, and finally to `reject` to prevent delivery of emails that fail DMARC checks altogether. This phased approach helps avoid disruptions in legitimate email traffic while refining the authentication processes.

01

Enhances Email Security
DMARC helps prevent attackers from using your domain to send malicious or fraudulent emails.

02

Protects Brand Reputation
DMARC helps protect your brand's integrity and trustworthiness. When customers receive genuine communications from your domain, their trust in your brand is upheld.

03

Improves Email Deliverability
DMARC policies can increase the likelihood that legitimate emails will be correctly identified and delivered to recipients' inboxes, rather than being marked as spam or rejected altogether.

04

Provides Insight through Reporting
DMARC includes a reporting function that sends reports back to the domain owner about messages that pass and fail DMARC evaluation. These reports provide valuable insights into email performance and potential security threats.

05

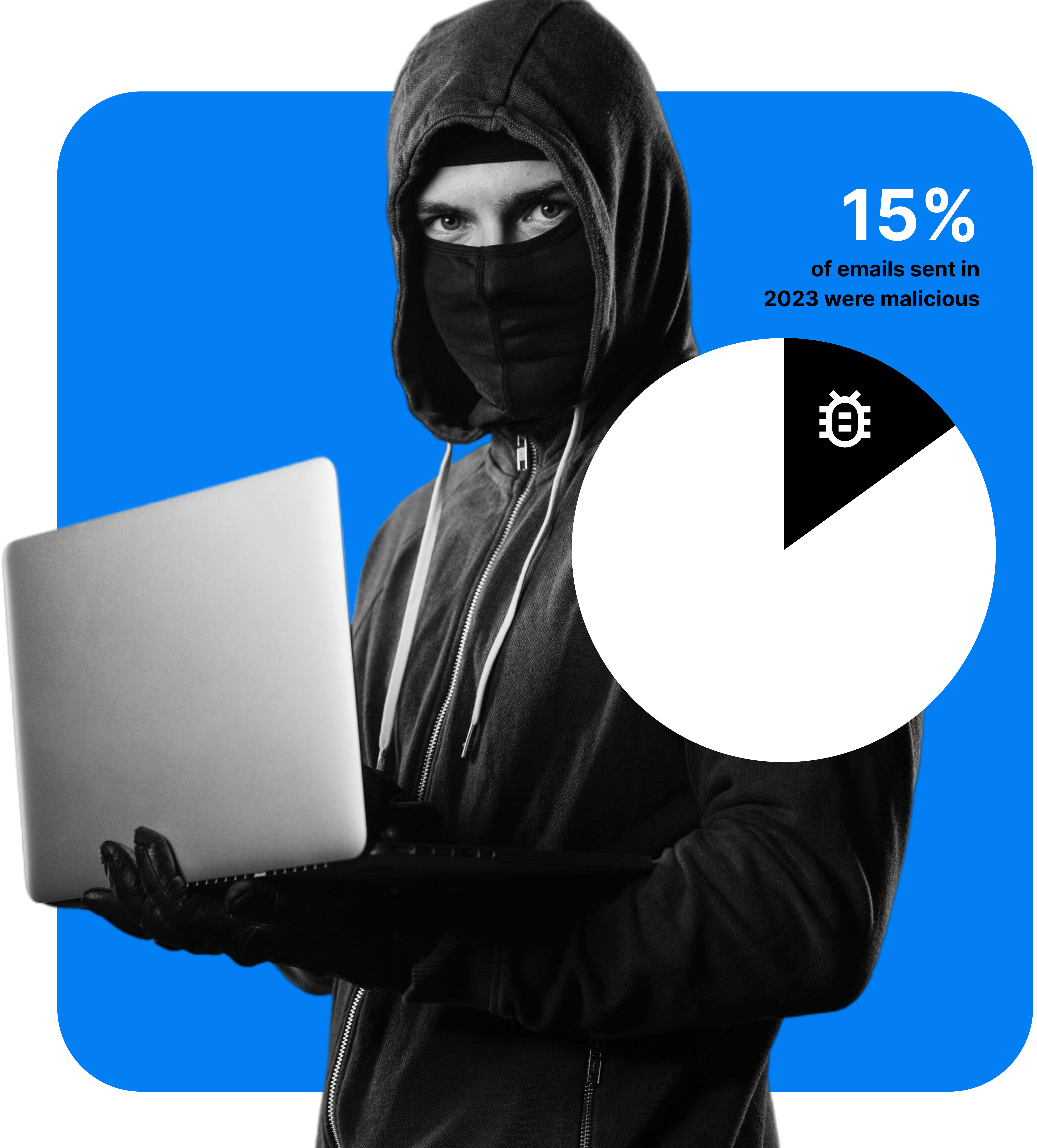
Regulatory Compliance
For certain industries, maintaining a secure and authenticated email environment may be part of regulatory compliance requirements.

2024 Email Send Requirements

The recent regulations set a new standard for businesses that send over 5,000 emails daily to Google and Yahoo! accounts. Effective February 2024, these regulations mandate the implementation of an active DMARC policy. Microsoft recently announced similar plans to enforce tough email authentication rules. This move aims to strengthen the security framework around email communications, significantly reducing the risk of phishing, spam, and cyber fraud.

Staying Ahead of Cyber Threats

According to a report by VIPRE Security Group, **15 percent of all emails sent in 2023 were malicious**, and that number is expected to rise. The need to secure emails is urgent should organizations expect to maintain current levels of business continuity. With cyber threats becoming more sophisticated, DMARC provides a critical defense mechanism. It empowers organizations to take control of their email security, significantly reducing the likelihood of email-based attacks.



15%

of emails sent in 2023 were malicious

The Future of Email Security

The landscape of email security is evolving rapidly. DMARC is at the forefront of this evolution, offering a robust framework for protecting email communications. Organizations must proactively adapt to these changes, ensuring their email practices are secure, compliant, and aligned with the best practices in cybersecurity.

A Strategic Approach to Defending Email Communications

Adopting DMARC policies can be complex, especially for large organizations with extensive email operations. DMARC regulations are more than a compliance requirement; they represent a proactive approach to protecting digital communications. As online brand impersonation and email-based attacks continue to rise, adopting DMARC is beneficial and essential for maintaining the integrity and security of email communication. By understanding and implementing DMARC, organizations can protect their brand, promote customer trust, and contribute to a safer digital ecosystem.

Setting Up DMARC

Implementing DMARC involves a multi-step process.

1

Initial SPF and DKIM Configuration:

Establishing SPF and DKIM records for a domain is the foundational step. SPF (Sender Policy Framework) records list authorized IP addresses for sending emails, while DKIM (DomainKeys Identified Mail) adds an encrypted signature to email headers.

By verifying that the email message truly comes from the domain it claims to represent and that the integrity of the message has been maintained, DKIM adds a layer of authentication that helps to build trust in email communications. DKIM uses a form of email signing to verify that an email message was not altered in transit between sending and receiving servers, thereby helping to establish the authenticity of the sender.

2

Creating a DMARC Policy:

A DMARC policy instructs email receivers on handling emails failing SPF or DKIM checks.

The policies include:

- **None:** The email is delivered normally, disregarding SPF or DKIM failures.
- **Quarantine:** The email is directed to the spam folder or a specified quarantine area.
- **Reject:** The email is not delivered at all. ***This is the ideal policy.***

3

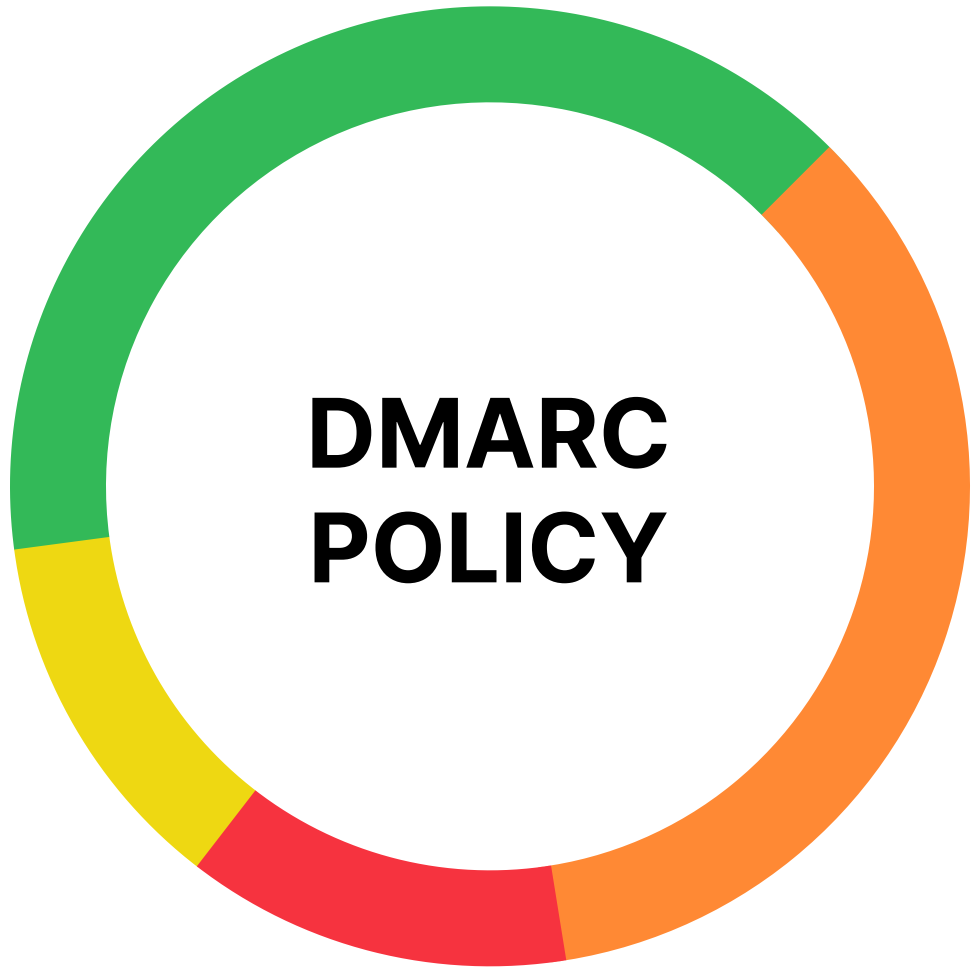
Monitoring and Reporting

Setting up effective reporting mechanisms under DMARC will be essential. These reports provide insights into the DMARC policy's performance, highlighting authenticated emails and identifying potential security threats.

Research Results

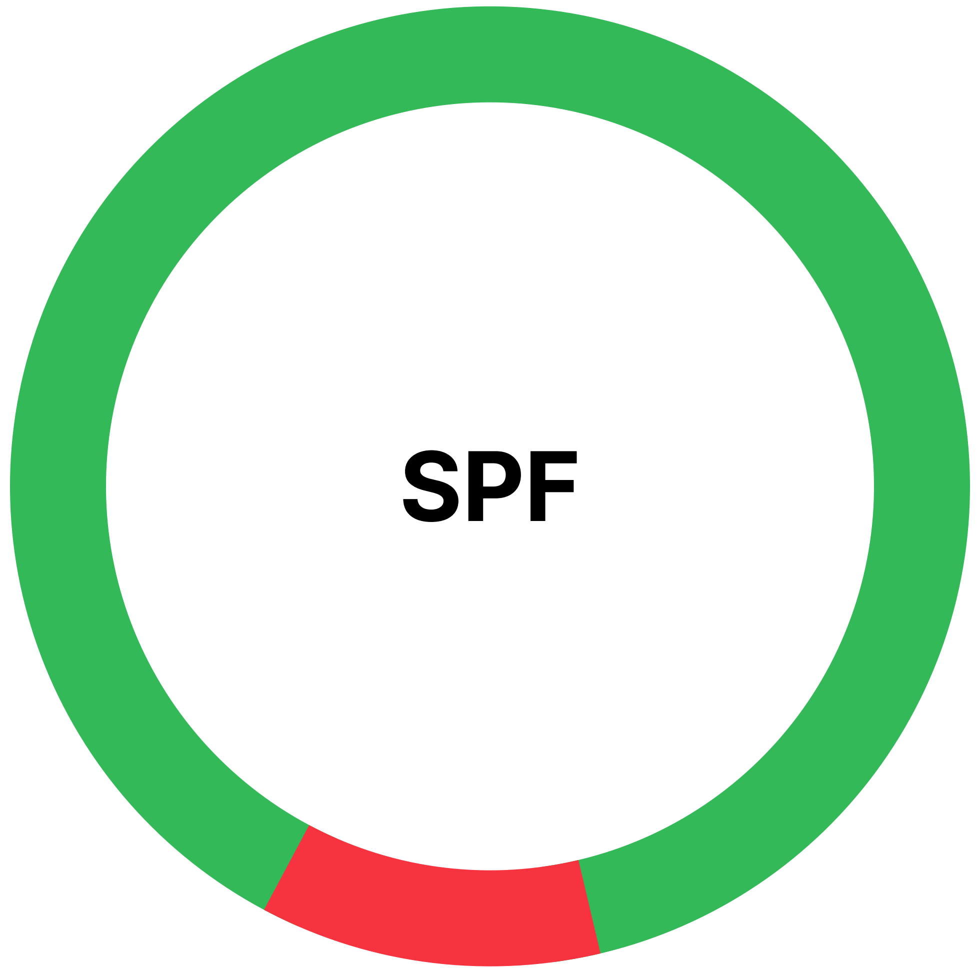
Most organizations in both states revealed a weak DMARC policy which aligns with the national trend. There is an opportunity to strengthen email security in the region.

Massachusetts DMARC Statistics



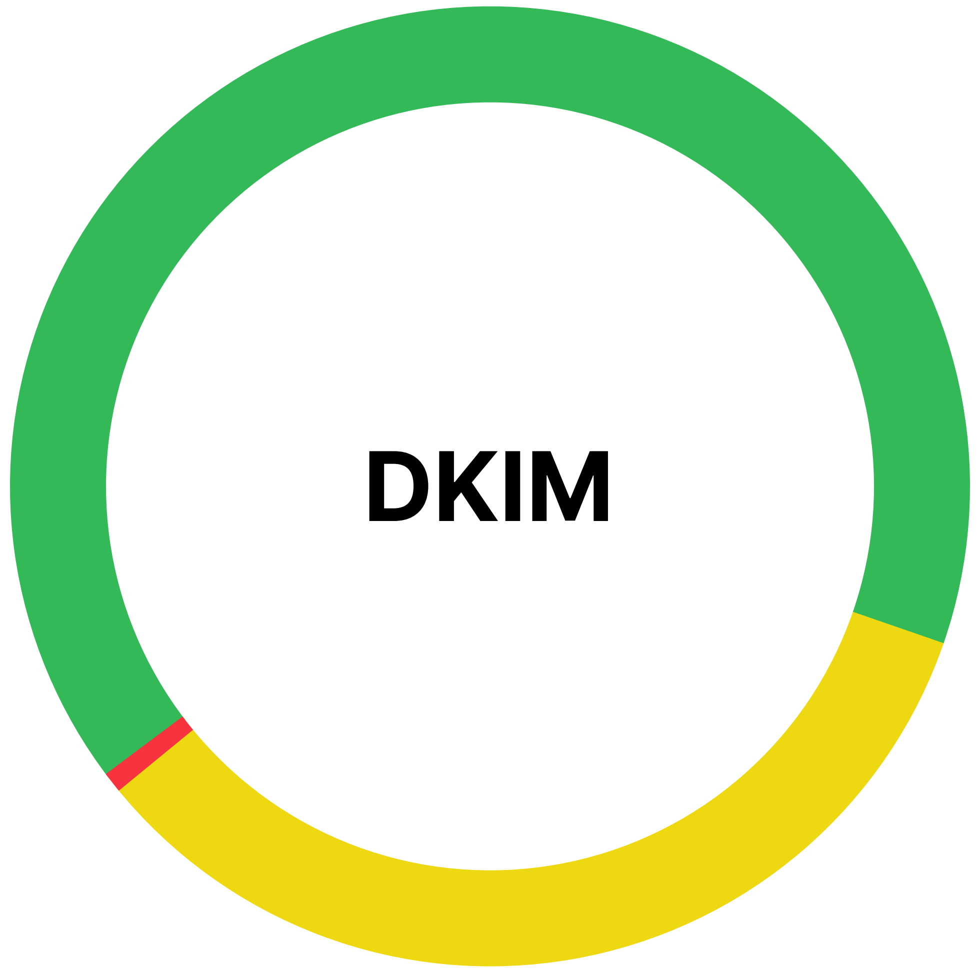
DMARC POLICY

🟥	No Valid DMARC Record	26 (13%)
🟧	None	71 (35.5%)
🟨	Quarantine	25 (12.5%)
🟩	**Reject**	**78 (39%)**



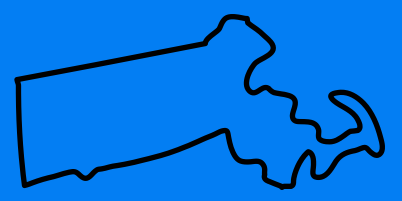
SPF

🟥	Invalid	23 (11.5%)
🟩	Valid	177 (88.5%)

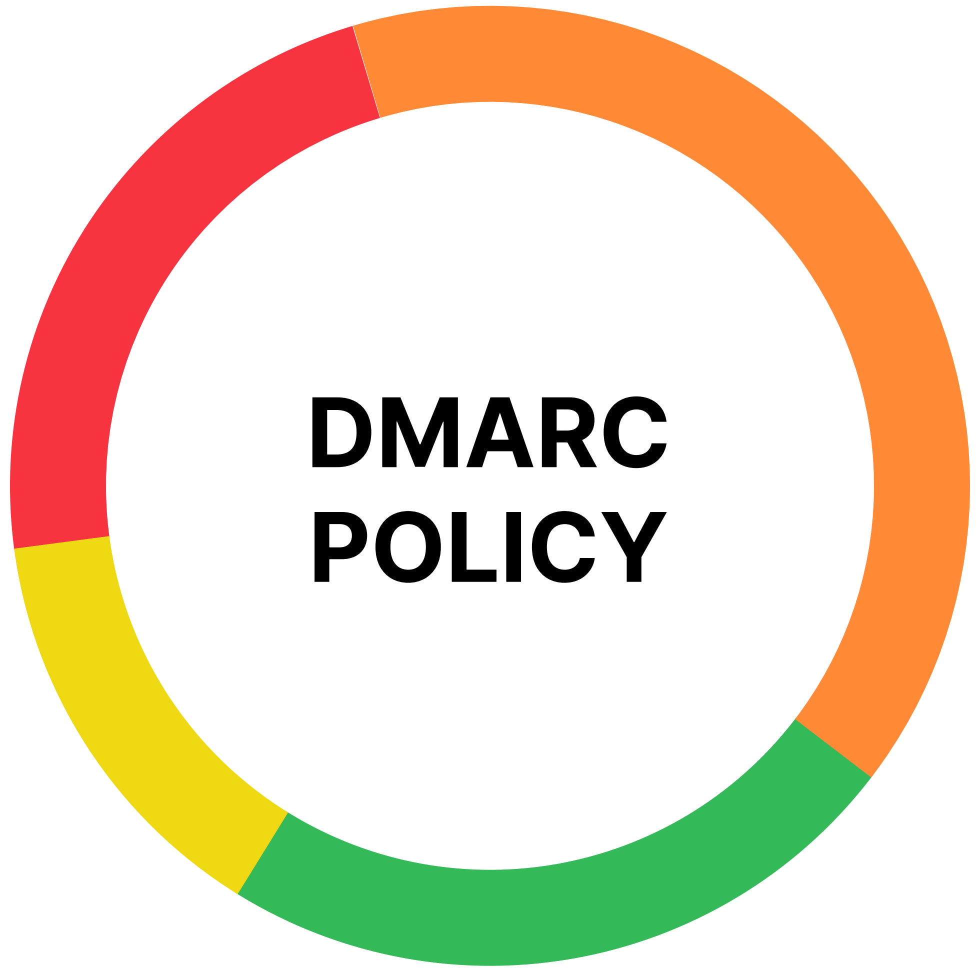


DKIM

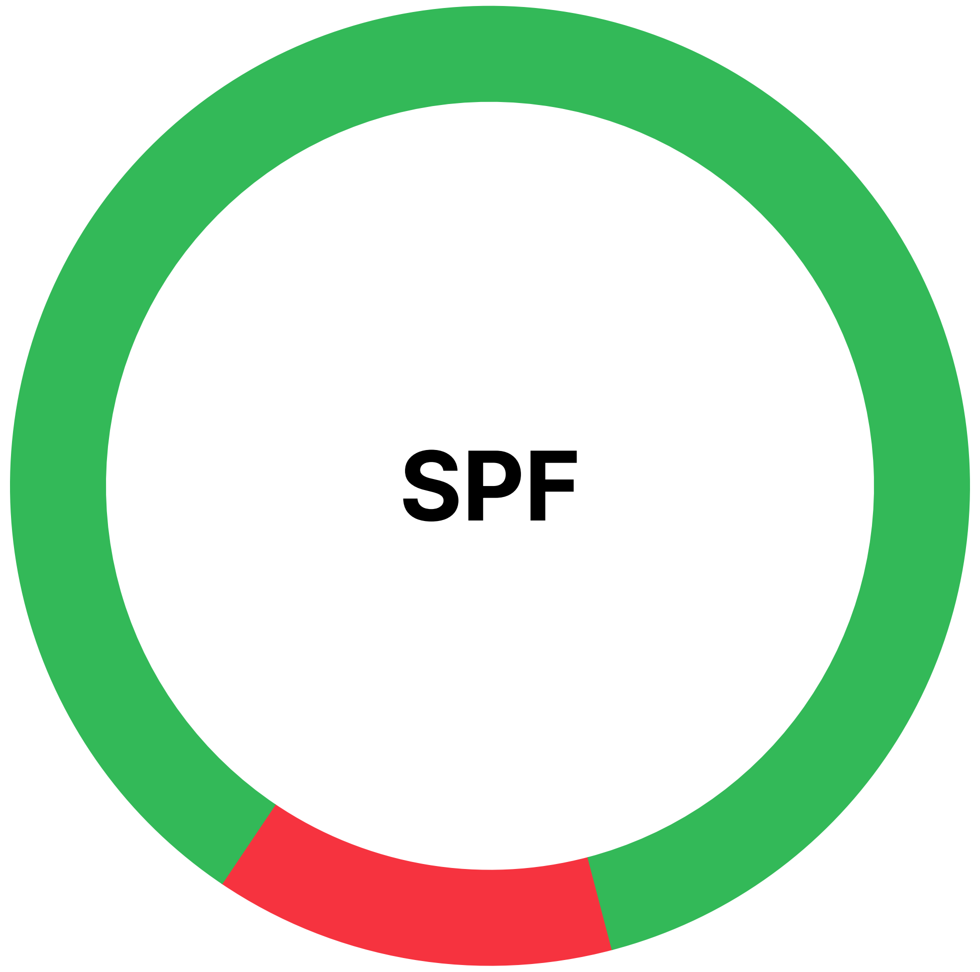
🟥	Invalid	1 (.5%)
🟨	Not Configured	68 (34%)
🟩	Valid	131 (65.5%)



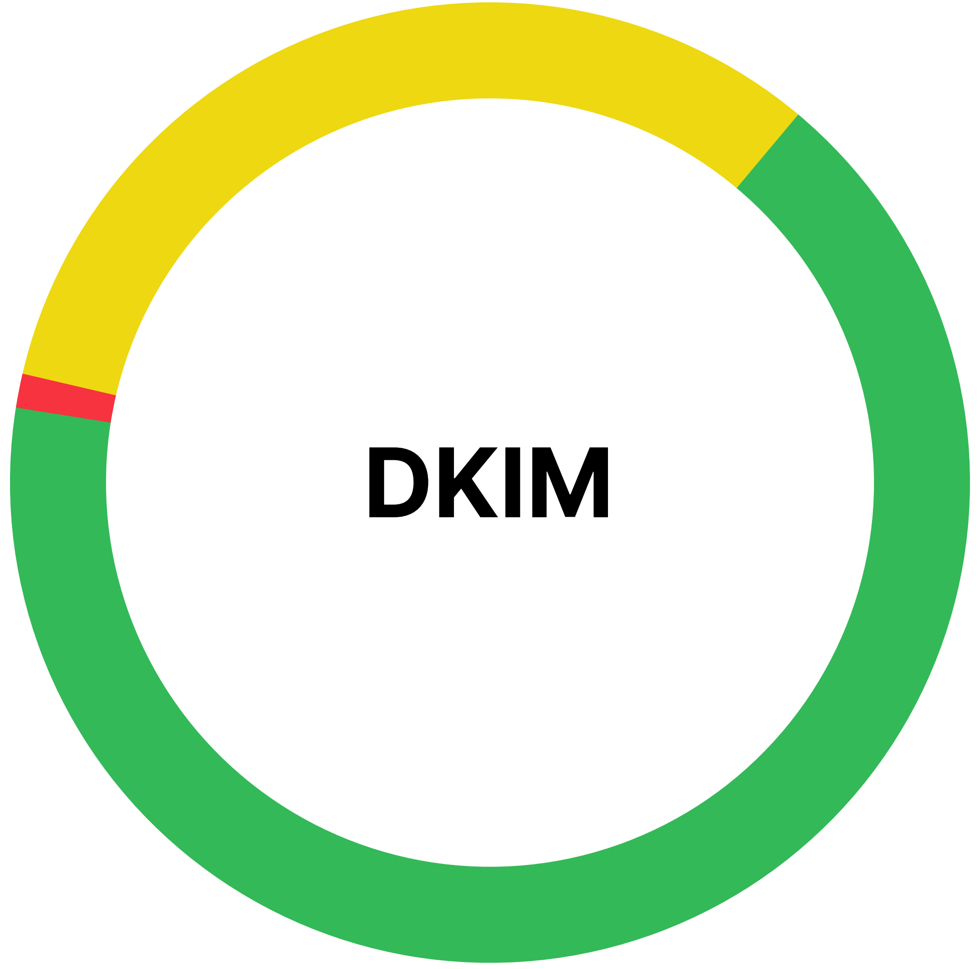
Rhode Island DMARC Statistics



🔴	No Valid DMARC Record	45 (22.5%)
🟠	None	80 (40%)
🟡	Quarantine	28 (14%)
🟢	**Reject**	**4 (23.5%)**



🔴	Invalid	27 (13.5%)
🟢	Valid	173 (86.5%)



🔴	Invalid	2 (1%)
🟡	Not Configured	65 (32.5%)
🟢	Valid	133 (66.5%)

After DMARC – What’s Next?

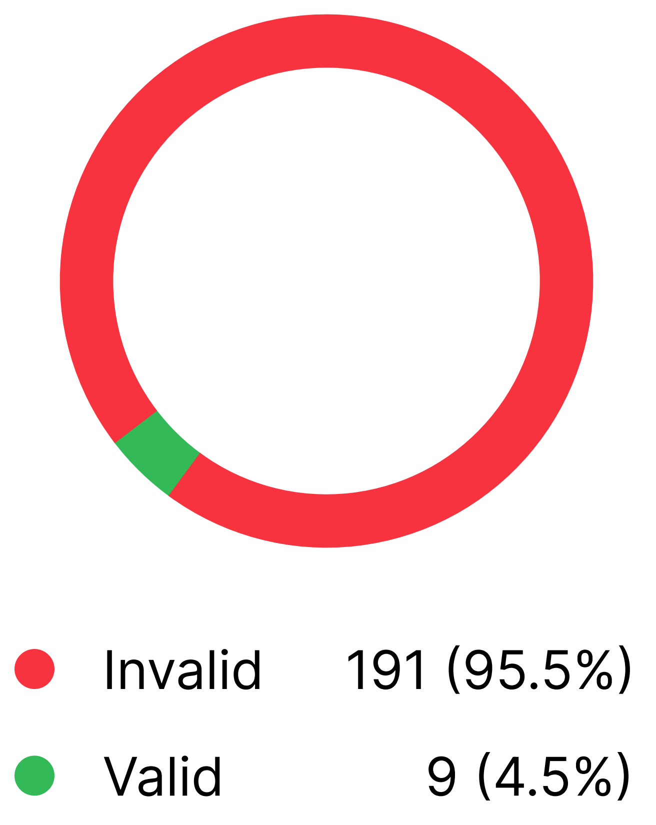
DMARC is a standard that has been around for over a decade, and organizations are beginning to put in the resources to meet this standard. While DMARC is a baseline in email security, there are additional standards recently developed that will further secure email communications. Some of these are simple to implement, and it can be expected that more organizations will adopt these standards. Out of the 400 domains reviewed, Remi IT Solutions found that email security policies such as BIMI, MTA-STS and TLS-RPT are virtually unused in both Rhode Island and Massachusetts.

BIMI: Your Logo Next to Your Emails

BIMI, which stands for Brand Indicators for Message Identification, is an email authentication standard that allows the display of brand-controlled logos alongside authenticated email messages in customers' inboxes. This standard works by leveraging a brand's existing DMARC implementation to add a visual element of trust and brand recognition to email communications. For BIMI to function, a domain must first have a DMARC policy of “quarantine” or “reject” set up. This ensures that the email domain is protected against unauthorized use and spoofing.

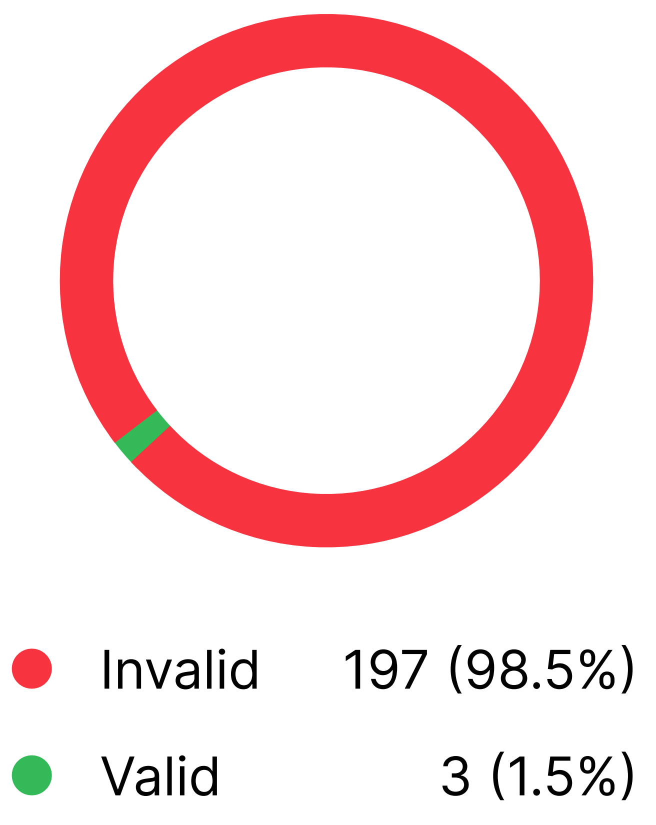
BIMI represents an evolution in email marketing and security, enhancing the effectiveness of existing standards like SPF, DKIM, and DMARC by adding a layer of brand visibility and trust. It is particularly valuable for organizations looking to improve their email engagement and protect their brand reputation.

MASSACHUSETTS



Massachusetts BIMI Record

RHODE ISLAND

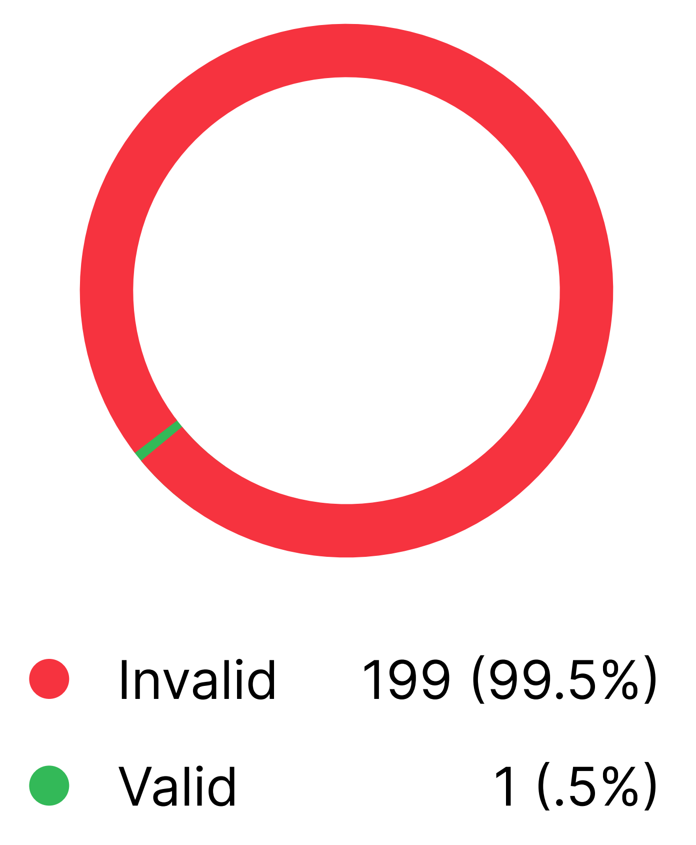


Rhode Island BIMI Record

MTA-STS: Forces Encryption Between Email Servers

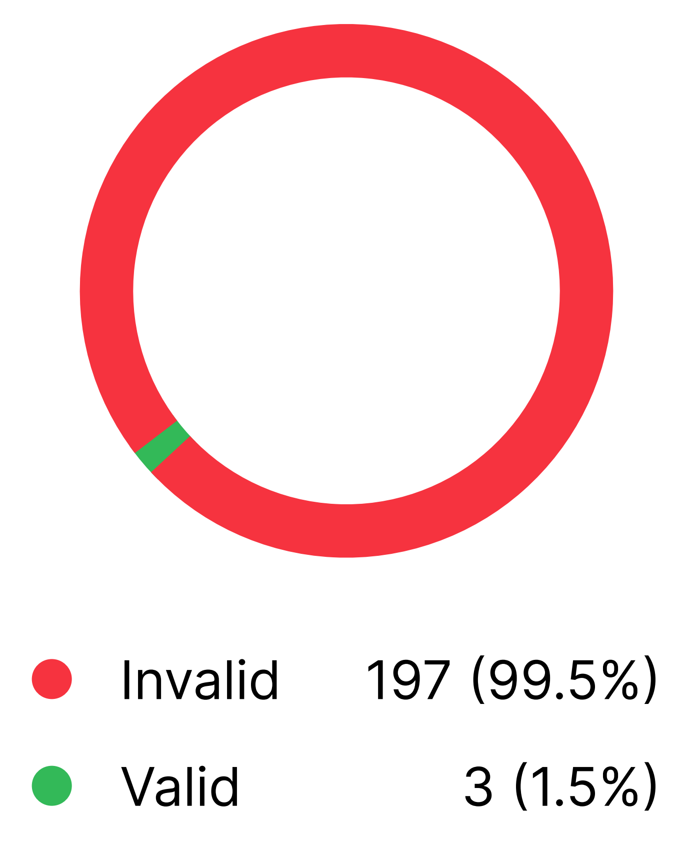
MTA-STS (Mail Transfer Agent Strict Transport Security) is an email security protocol designed to enhance the security of SMTP (Simple Mail Transfer Protocol) connections by enabling mail service providers to declare their ability to receive Transport Layer Security (TLS) secure connections. If set up correctly, it enforces encrypted connections and rejects connections that are not encrypted. MTA-STS reduces the risk of man-in-the-middle attacks during email transmission.

MASSACHUSETTS



Massachusetts MTA-STS Record

RHODE ISLAND



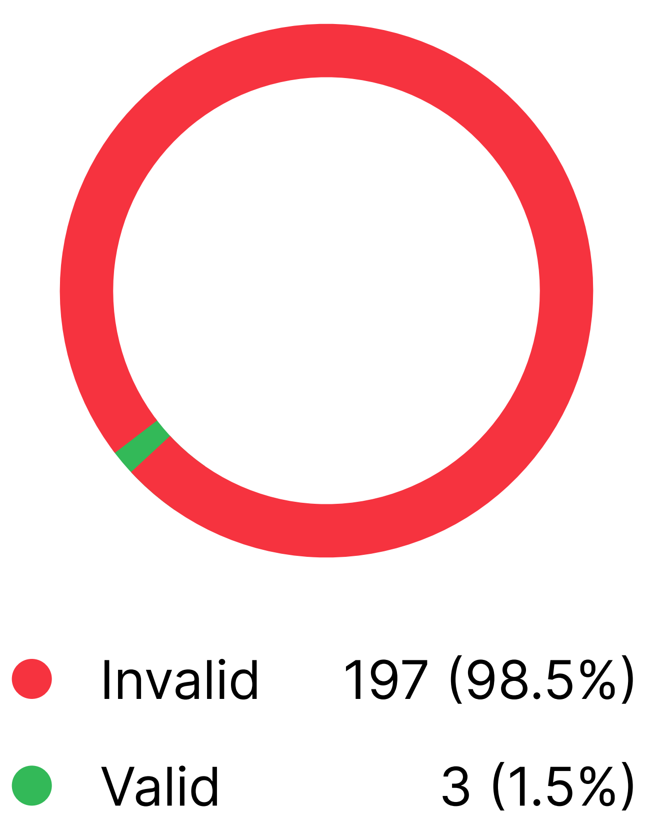
Rhode Island MTA-STS Record

TLS-RPT: The Reporting Mechanism for MTA-STS

TLS-RPT, or TLS Reporting, is a standard that complements the MTA-STS by providing a mechanism for reporting on the success and failure of email transport security attempts. Officially known as SMTP MTA-STS and TLS Reporting, this protocol helps domain owners monitor and troubleshoot issues related to the delivery of emails over secure connections.

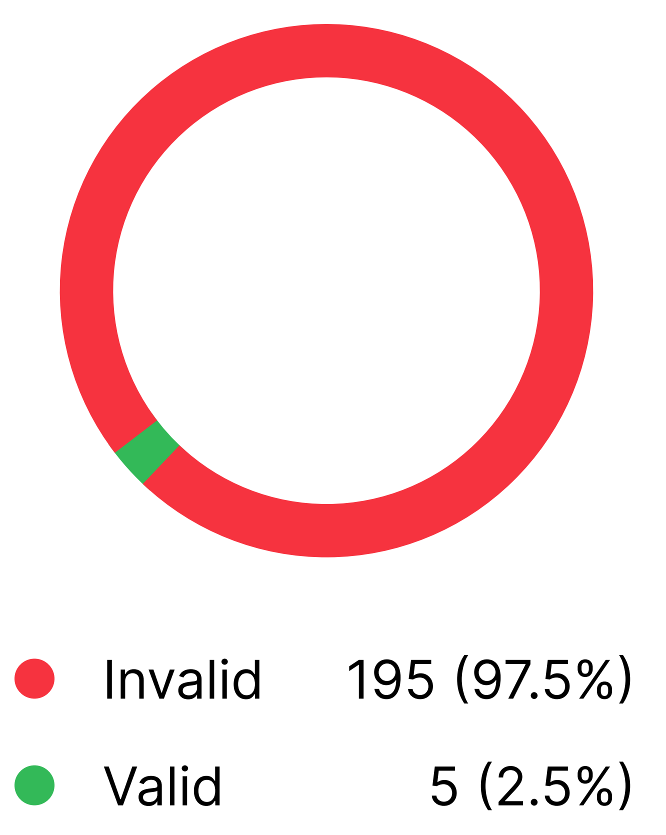
TLS-RPT enhances the security framework provided by MTA-STS by adding transparency and accountability. It helps organizations ensure that their email transport security configurations are functioning as intended and assists in identifying potential security issues affecting email delivery.

MASSACHUSETTS



Massachusetts TLS-RPT Record

RHODE ISLAND

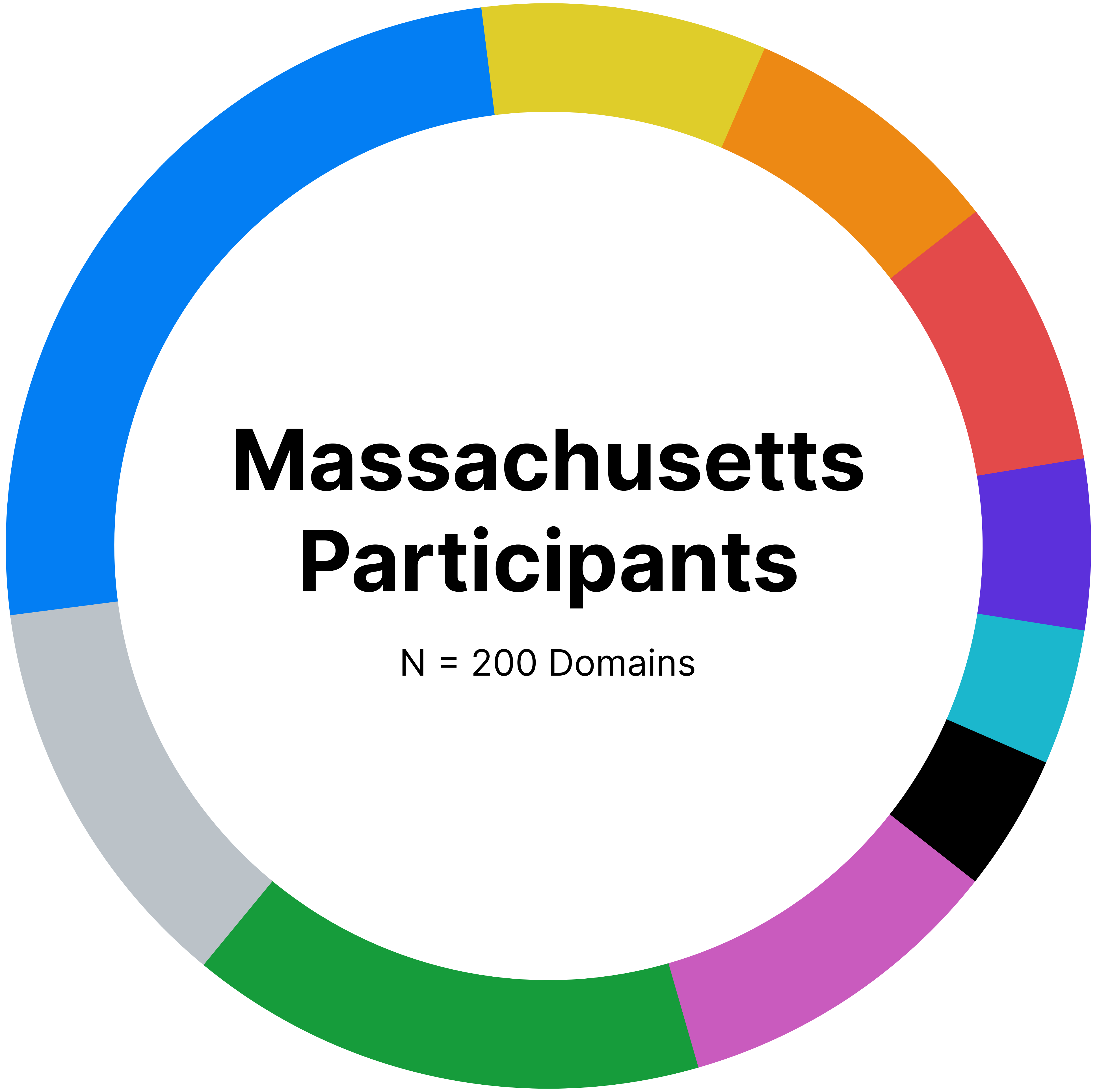


Rhode Island TLS-RPT Record

Participants and Methodology

Using publicly available data and data pulled from a subscription-based marketing research service, Remi IT Solutions compiled a list of 200 of the largest organizations by estimated annual revenue for Massachusetts, and then for Rhode Island. The research for the 200 email domains for organizations in Massachusetts was conducted on April 4, 2024.

The research for the 200 email domains in Rhode Island was conducted on April 10, 2024 and May 16, 2024. Remi IT Solutions analyzed the 400 domains for the following characteristics: DMARC policy, SPF, DKIM, BIMI, MTA-STS, and TLS-RPT.



Massachusetts Participants

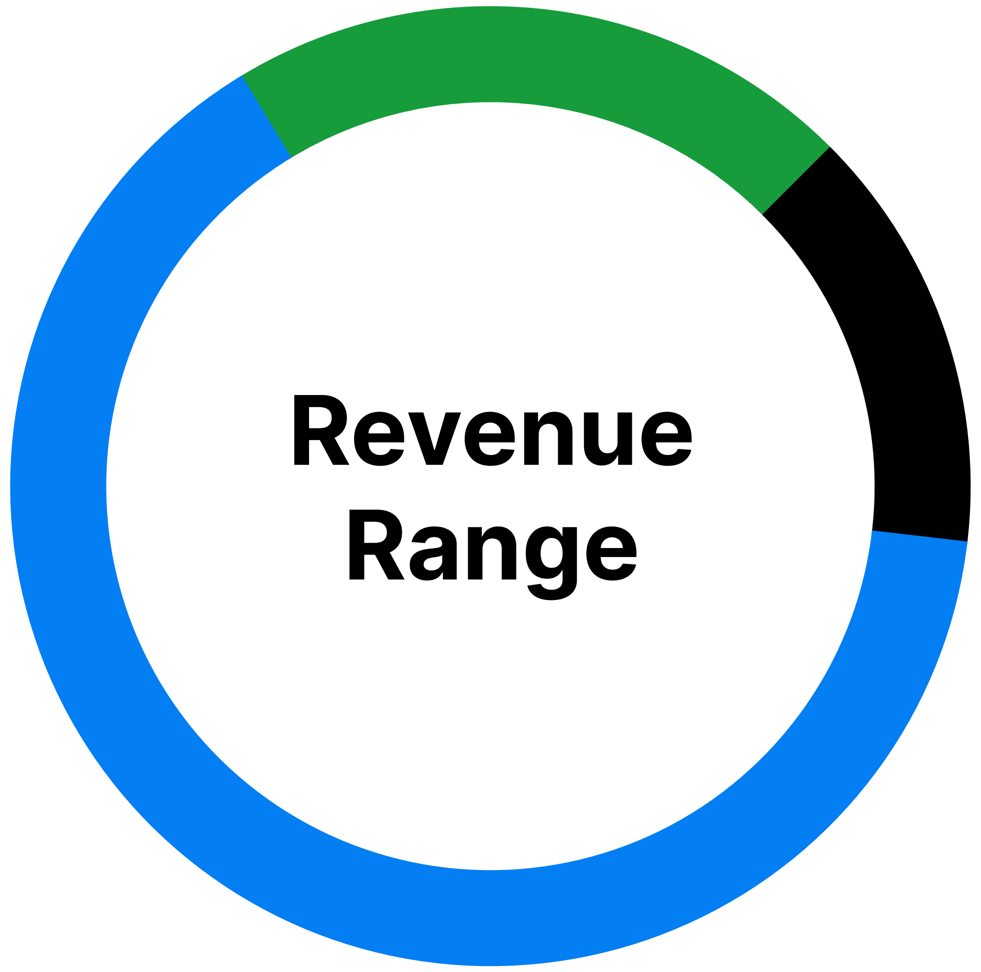
N = 200 Domains

Primary Industry

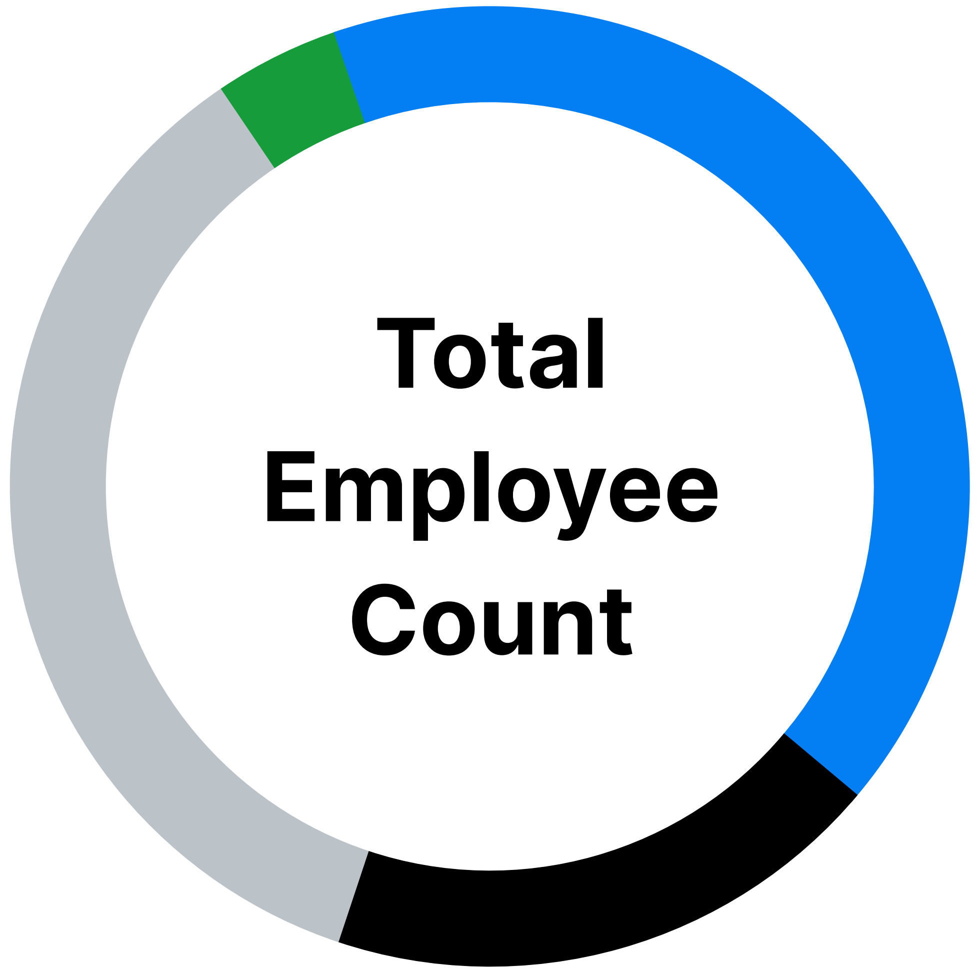
●	Finance	4%
●	Energy, Utilities, & Waste	4%
●	Education	5%
●	Business Services	12%
●	Healthcare	8%
●	Insurance	10%
●	Manufacturing	25%
●	Retail	8.5%
●	Software	8%
●	Other	15.5%

Massachusetts Participants

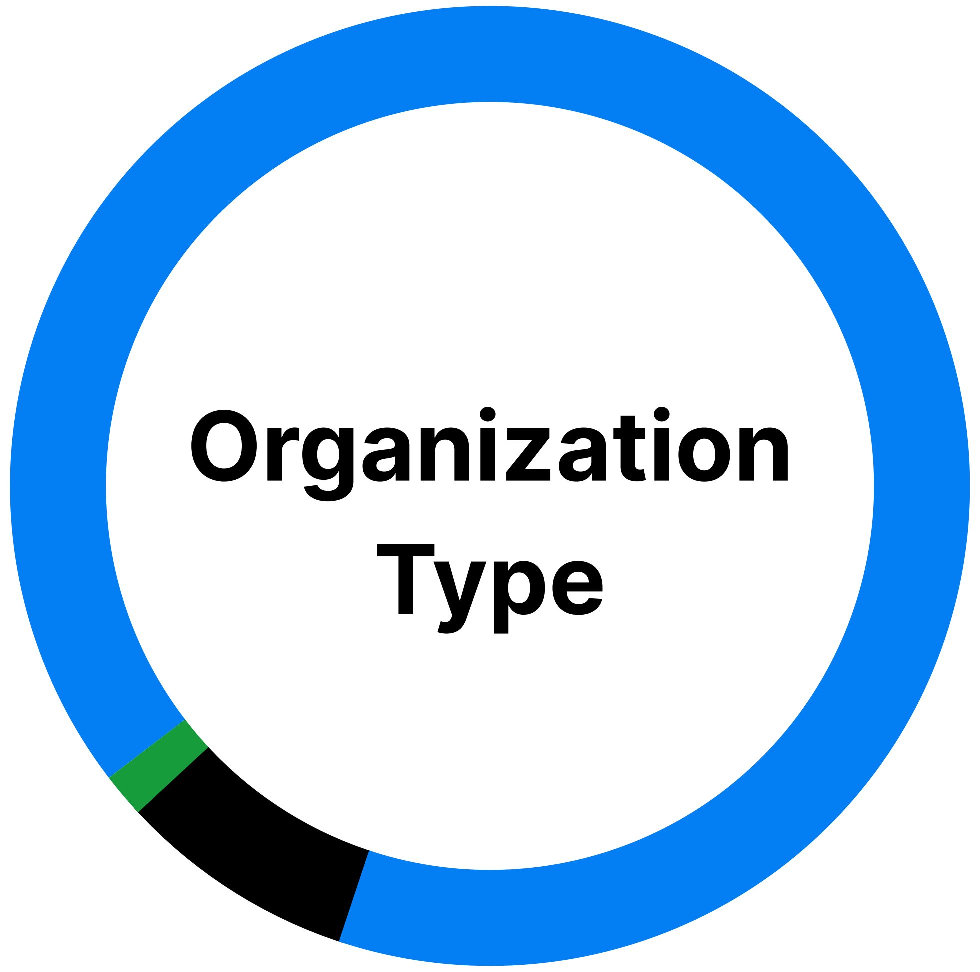
N = 200 Domains



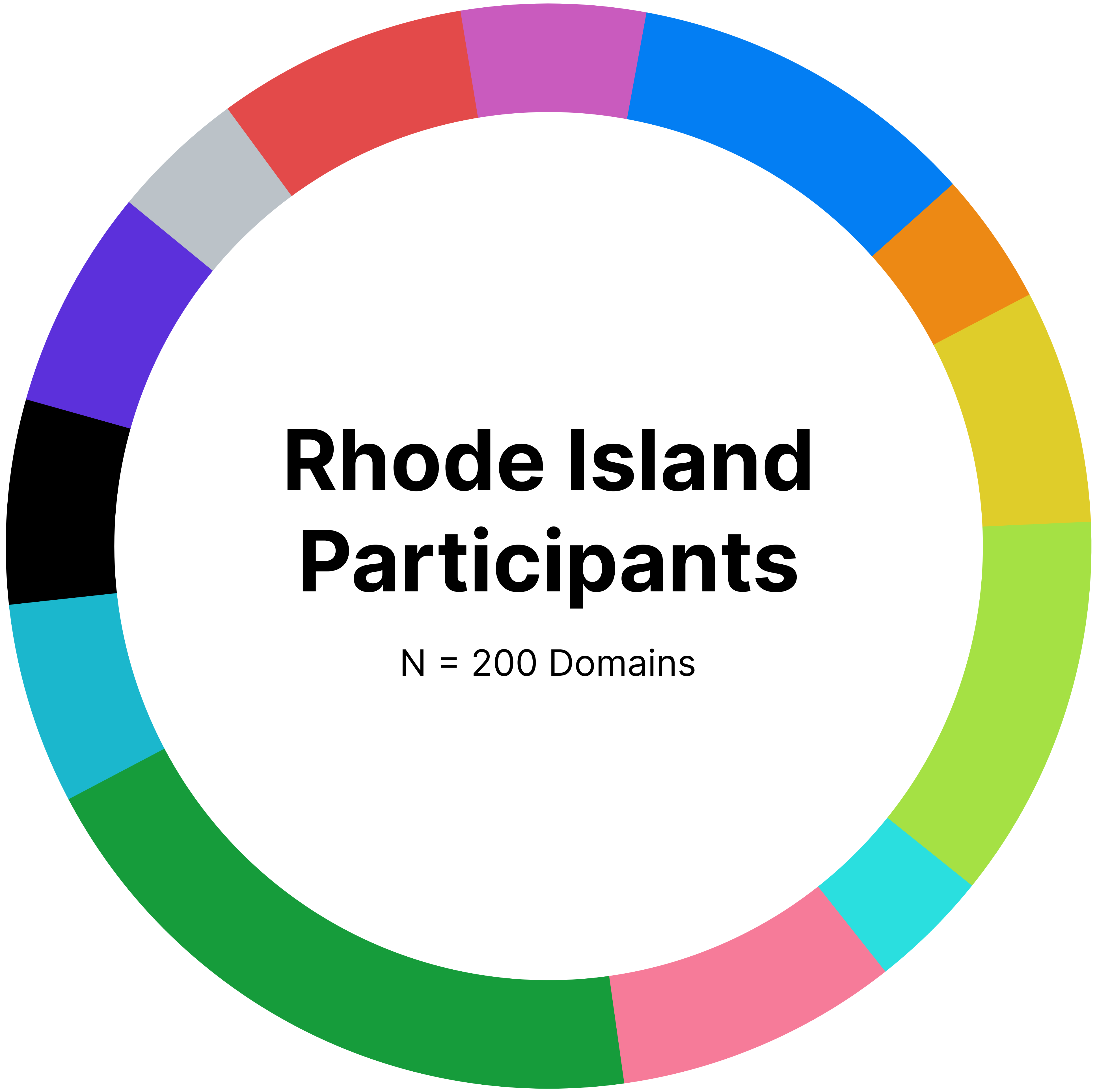
●	$500 mil - $1 bil	14.5%
●	$1bil - $5 bil	64.5%
●	Over $5 bil	21%



●	500-999 Employees	4.5%
●	1,000 - 4,999 Employees	41%
●	5,000 - 9,999 Employees	19%
●	10,000+ Employees	35.5%



●	B2B	90.5%
●	B2C	8%
●	Government	1.5%



Rhode Island Participants

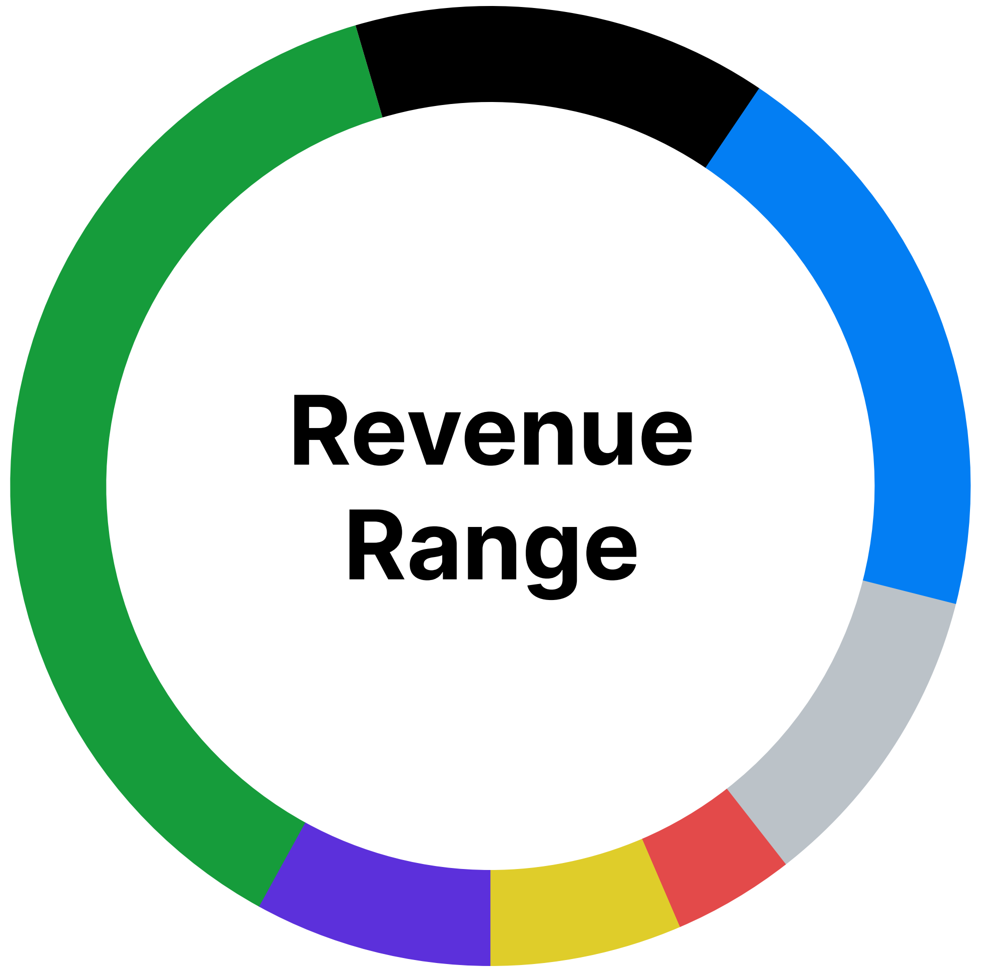
N = 200 Domains

Primary Industry

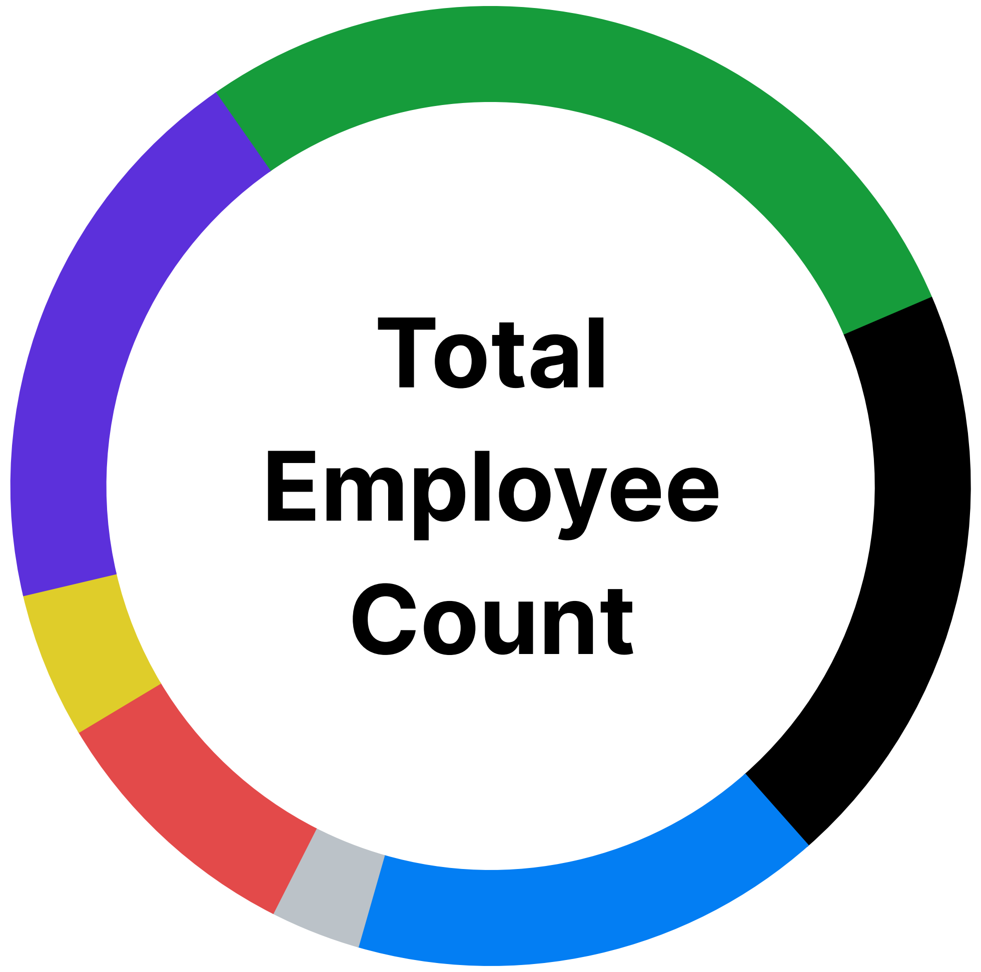
●	Business Services	6%
●	Construction	6%
●	Education	6.5%
●	Energy, Utilities & Waste	4%
●	Finance	7.5%
●	Government	5.5%
●	Healthcare	10.5%
●	Hospitality	4%
●	Insurance	7%
●	Manufacturing	19.5%
●	Other	11.5%
●	Real Estate	3.5%
●	Retail	8.5%

Rhode Island Participants

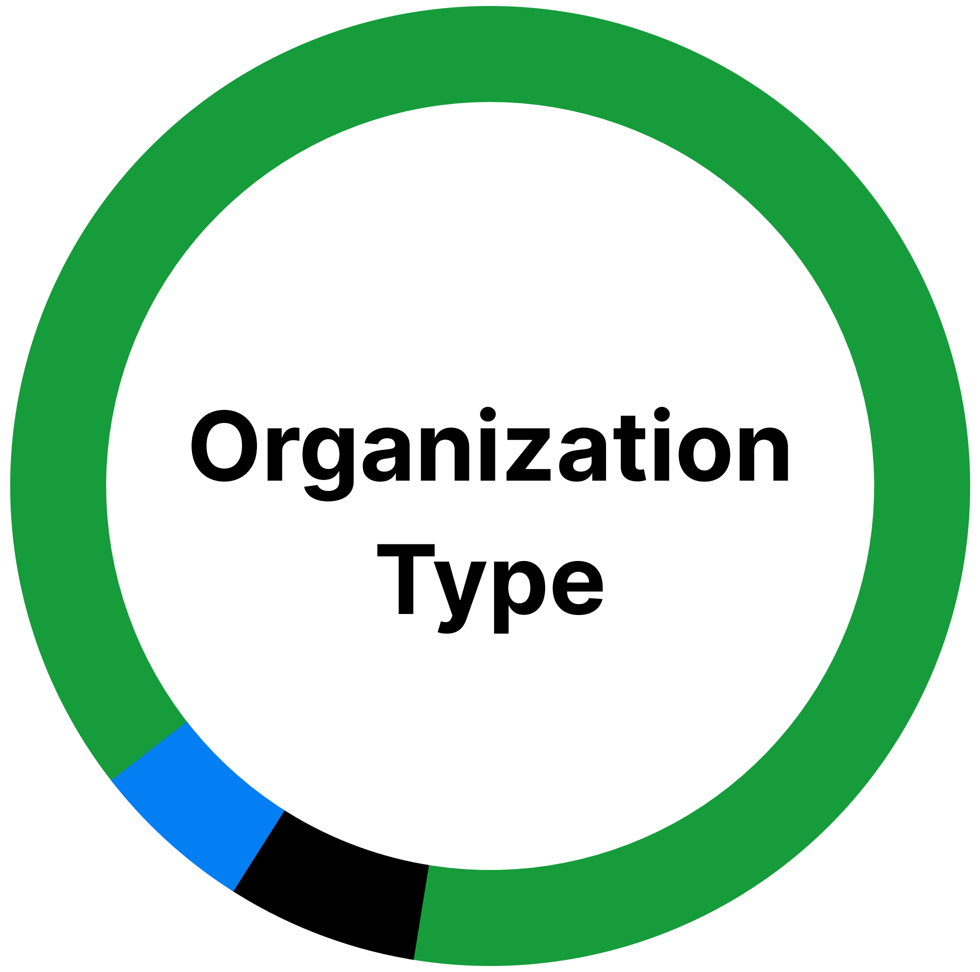
N = 200 Domains



⚫	$1 mil - $49 mil	14%
🟢	$50 mil - $99 mil	37.5%
🔵	$100 mil - $249 mil	19.5%
⚪	$250 mil - $499 mil	10.5%
🔴	$500 mil - $1 bil	4%
🟡	$1bil - $5 bil	6.5%
🟣	Over %5 bil	8%



🟡	20 - 99 Employees	5%
🟣	100 - 249 Employees	19%
🟢	250 - 499 Employees	28%
⚫	500 - 999 Employees	20%
🔵	1,000 - 4,999 Employees	16%
⚪	5,000 - 9,999 Employees	3%
🔴	10,000 Employees	9%



🟢	B2B	88%
⚫	B2C	6.5%
🔵	Government	5.5%

About Remi IT Solutions

Remi IT Solutions is on a mission to make IT easy for small and medium-sized businesses throughout Rhode Island and Massachusetts. Remi IT Solutions offers a cloud-forward, security-first approach to IT to help safeguard your business and optimize your IT investments. Headquartered in North Attleboro, Massachusetts with an office in Providence, Rhode Island, Remi IT Solutions proudly employs local IT professionals who will come onsite when needed.

Get Your Free DMARC Report
www.remi-it.com/Free-DMARC-Report →

Glossary

BIMI – Brand Indicators for Message Identification (BIMI) is an email authentication protocol that allows the display of brand-controlled logos next to authenticated email messages in customers' inboxes.

DKIM – DomainKeys Identified Mail, is an email authentication method designed to help protect email senders and recipients from email spoofing and phishing. DKIM verifies that the email is being sent by the intended sender and that the message was not tampered with during transit.

- **Invalid** – This status typically indicates that while a DKIM selector/s is/are present, there are problems with how it is implemented or configured.
- **Not Configured** – The domain is missing a DKIM selector.
- **Valid** – The DKIM selector/s on the email is/are correct and passed the verification process.

DMARC Policy – A DMARC policy specifically refers to the part of the DMARC protocol that domain owners set to instruct receiving email servers on how to deal with messages that fail DMARC authentication checks. This policy is defined within the DMARC record in the domain's DNS settings.

- **N (None)** – A DMARC policy of none (typically indicated as p=none in the DMARC record) indicates that the domain has DMARC verification enabled but is not taking any action against emails that fail DMARC checks. This policy is often used for monitoring and collecting data about the domain's email flows without affecting the delivery of emails, even if they fail DMARC checks. This is designed as a temporary step during the rollout of a secure DMARC policy.
- **No Valid DMARC Record** – These domains do not have a DMARC record that could be validated. Without a valid DMARC record, these domains are not able to specify how email receivers should handle emails that fail authentication checks, potentially increasing the risk of spoofing and phishing attacks.
- **Q (Quarantine)** – A DMARC policy of quarantine (indicated as p=quarantine) suggests that emails failing DMARC authentication should be treated suspiciously. Typically, this means such emails could be placed into the spam folder or undergo additional scrutiny. This policy is a step up from none, providing more protection against potentially harmful emails while still allowing them to be delivered to a place where they can be reviewed. While helpful, quarantine is not an ideal policy.
- **R (Reject)** – The reject policy (indicated as p=reject) is the strictest form of DMARC policy. It instructs email receivers to reject emails that fail DMARC checks outright. This prevents such emails from being delivered altogether, offering the highest level of protection against email spoofing and phishing. This is the ideal DMARC policy.

MTA-STS – MTA-STS is an email security protocol designed to enhance the security of SMTP (Simple Mail Transfer Protocol) connections by enabling mail service providers to declare their ability to receive Transport Layer Security (TLS) secure connections. If set up correctly, it enforces encrypted connections and rejects connections that are not encrypted. MTA-STS reduces the risk of man-in-the-middle attacks during email transmission.

- **Valid** – MTA-STS is configured.
- **Invalid –** MTA-STS is missing or misconfigured.

SPF – Sender Policy Framework (SPF) is an email authentication method designed to prevent spammers from sending messages on behalf of another’s domain. This protocol is used to ensure that emails claiming to come from a specific domain are authorized by the owner of that domain.

- **Valid** – The SPF record is configured correctly and has ten or fewer entries (sending sources).
- **Invalid** – The SPF is missing or not correctly configured (which can include more than 10 sending sources).

TLS-RPT – TLS Reporting (TLS-RPT) is a standard that complements the MTA-STS by providing a mechanism for reporting on the success and failure of email transport security attempts.

- **Valid** – TLS-RPT is configured correctly.
- **Invalid** – TLS-RPT is missing or misconfigured.