DMARC Adoption in Canada: 2021 Report

POWERDMARC

POWERDMARC

Case study

DMARC Adoption in Canada: 2021 Report

Assessing the Threat Landscape

- In the 2020 Cyberthreat Defense Report (CDR) it came to light that 78 percent of Canadian organizations experienced at least one cyber attack within a 12-month period, all of which were successful attacks.
- More than 70% of Canadian businesses faced Ransomware attacks between 2020-2021, making it the 6th most attacked country in the world in the past 1 year, with the average cost exceeding $400,000
- The report also highlighted the fact that only 74% of businesses in Canada support AI-based security solutions and email authentication practices
- Only a small percentage of Canadian companies (26%) were successful in setting up preventive measures against suspected Ransomware attacks
- In a Data Breach Report by IBM formulated in 2020, the average loss of financial assets dealt by Canadian organizations due to data breaches was estimated to be a whopping $4.5 million in the past 1 year
- In between 2020-2021, 525 Canadian organizations fell prey to spear-phishing scams which led to the loss of $14.4 million in assets
- Phishing attacks and fake email scams spiked up considerably in the COVID and post-COVID conditions

The above-mentioned statistics on ransomware, data breaches, and phishing attacks in Canada over the course of the past 1 year, raise some serious concerns:

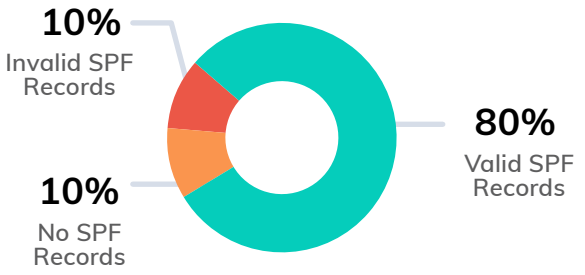
- What is the current situation of DMARC adoption and enforcement in organizations in Canada?
- How can we improve the cybersecurity and email authentication infrastructure in Canada to mitigate impersonation attacks?

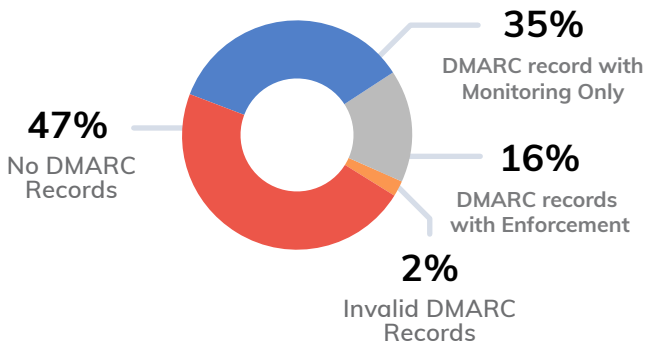
To gain better insight into the current scenario we analyzed 140 domains belonging to top businesses and organizations in Canada, from the following sectors:

- Energy
- Education
- Telecom
- Healthcare
- Transport
- Media & Entertainment
- Banking and Finance

What Do the Numbers Say?

An in-depth SPF and DMARC adoption analysis was conducted while examining all 140 Canadian domains, which led to the following revelations:



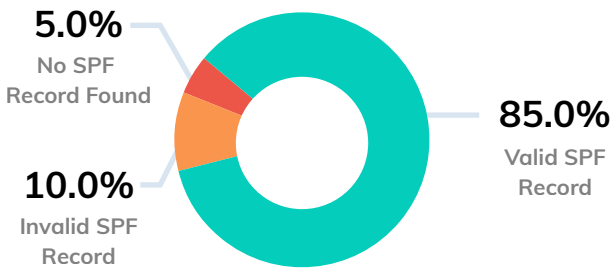


- Graphical Analysis: Among all 140 domains examined that belong to various organizations in Canada, 126 domains (90%) possessed SPF records, out of which 14 domains (10%) had SPF records with errors. Only 74 domains (52.8%) had DMARC records out of which 3 of the domains (2.14%) contained errors. 49 domains had their DMARC policy set at none (35%), enabling monitoring only, while 22 domains (15.7%) had their DMARC policy level set at enforcement (i.e. p=quarantine/reject).

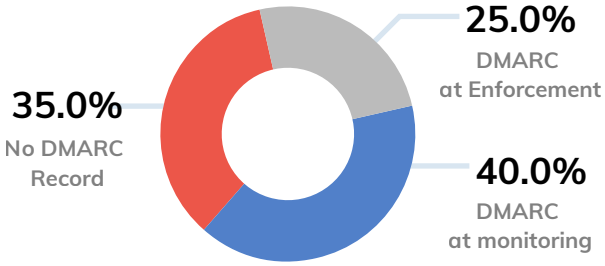
Sector-wise Analysis of Canadian Domains

Energy Sector

SPF Adoption Rate in the Canadian Energy Sector



DMARC Adoption Rate in the Canadian Energy Sector

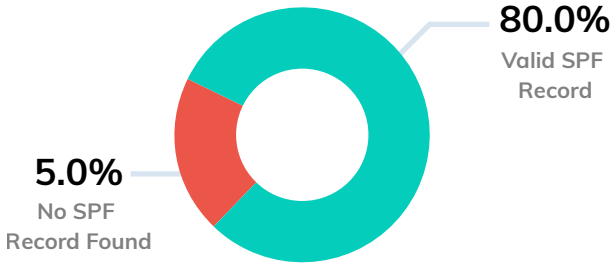


Key Findings:

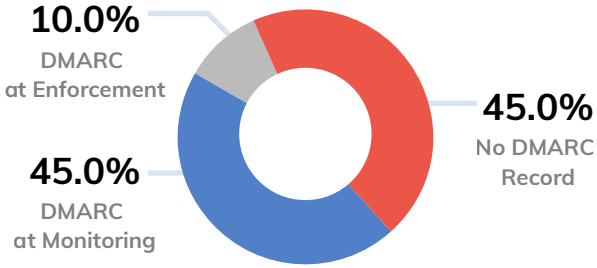
- 10% of the total domains in the Canadian energy sector possessed invalid SPF records
- Only 25% of the total domains had DMARC at an enforcement level of p=quarantine/reject
- No DMARC record was found in 45% of the domains

Telecom Sector

SPF Adoption Rate in the Canadian Telecom Sector



DMARC Adoption Rate in the Canadian Telecom Sector

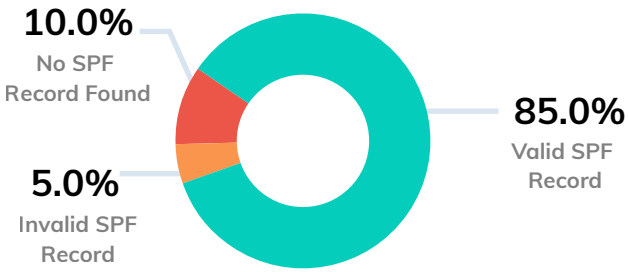


Key Findings:

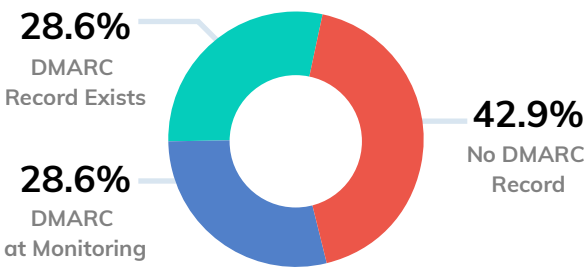
- 20% of the total domains in the Canadian Telecom sector had no SPF record published on their DNS
- Only 10% of the total domains had DMARC at an enforcement level of p=quarantine/reject
- While 45% of the domains had no DMARC record published on their DNS

Education Sector

SPF Adoption Rate in the Canadian Education Sector



DMARC Adoption Rate in the Canadian Education Sector

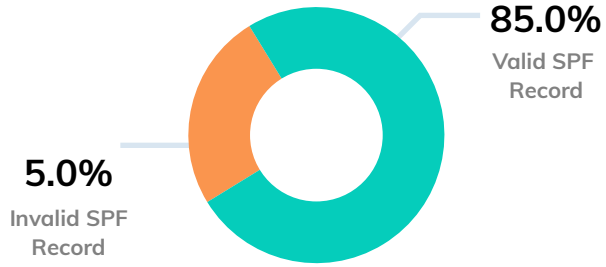


Key Findings:

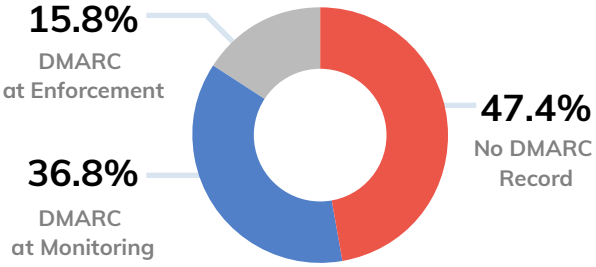
- 85% of the domains in the Canadian Education Sector had valid SPF records published on their domain's DNS
- However, only 28.6% of the domains contained a DMARC record in their DNS, all of which were at monitoring only (at p=none)

Healthcare Sector

SPF Adoption Rate in the Canadian Healthcare Sector



DMARC Adoption Rate in the Canadian Healthcare Sector

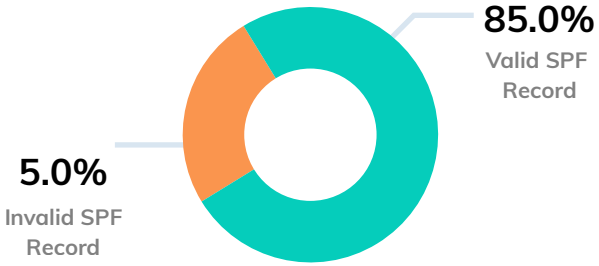


Key Findings:

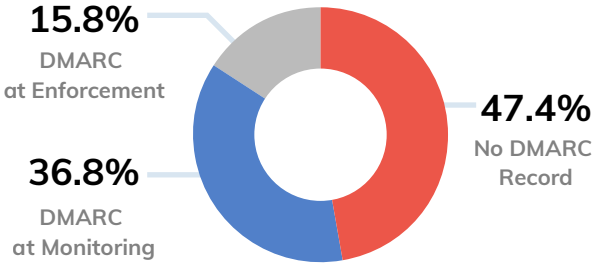
- 75% of the total domains in the Canadian Healthcare sector contained valid SPF records while 15% of the total domains didn't have any SPF record in their DNS
- Only 15% of the domains had their DMARC record set at an enforcement level of p=quarantine/reject
- 45% of the domains had no DMARC record published on their DNS

Transport Sector

SPF Adoption Rate in the Canadian Transport Sector



DMARC Adoption Rate in the Canadian Transport Sector

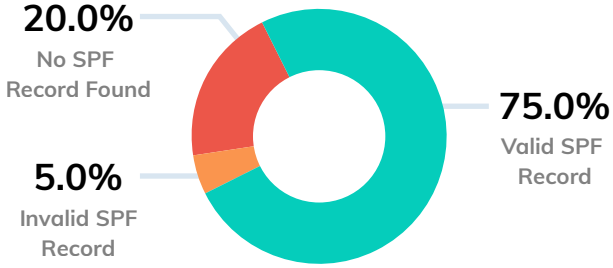


Key Findings:

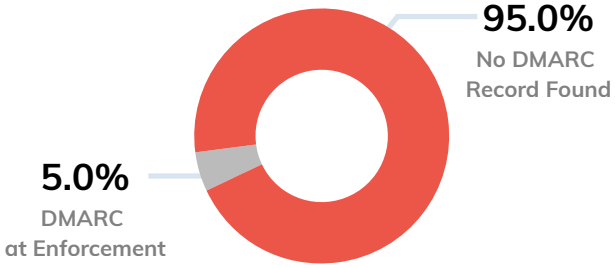
- 25% of the domains in the Canadian transport sector had SPF records that contained errors which rendered them invalid and ineffective
- No DMARC record was found in the DNS of 47.4% of the domains
- Only 15.8% of the domains were at DMARC enforcement

Media and Entertainment Sector

SPF Adoption Rate in the Canadian Media and Entertainment Sector



DMARC Adoption Rate in the Canadian Media and Entertainment Sector

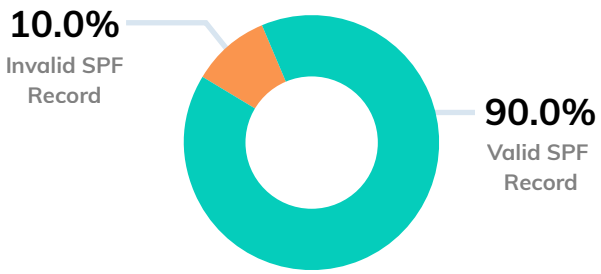


Key Findings:

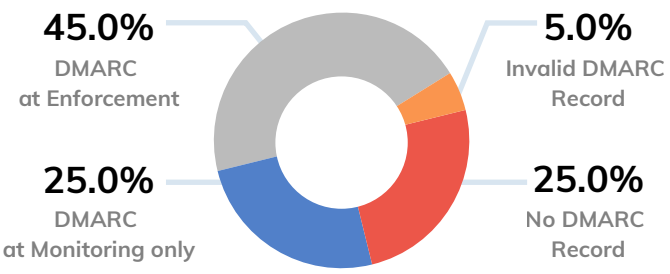
- 20% of the domains in the Canadian Media and Entertainment sector contained no SPF record in their domain's DNS
- Out of the 80% domains that contained an SPF record, 5% of the records contained errors
- Only 5% of the domains were at DMARC enforcement

Banking and Finance Sector

SPF Adoption Rate in the Canadian Finance Sector



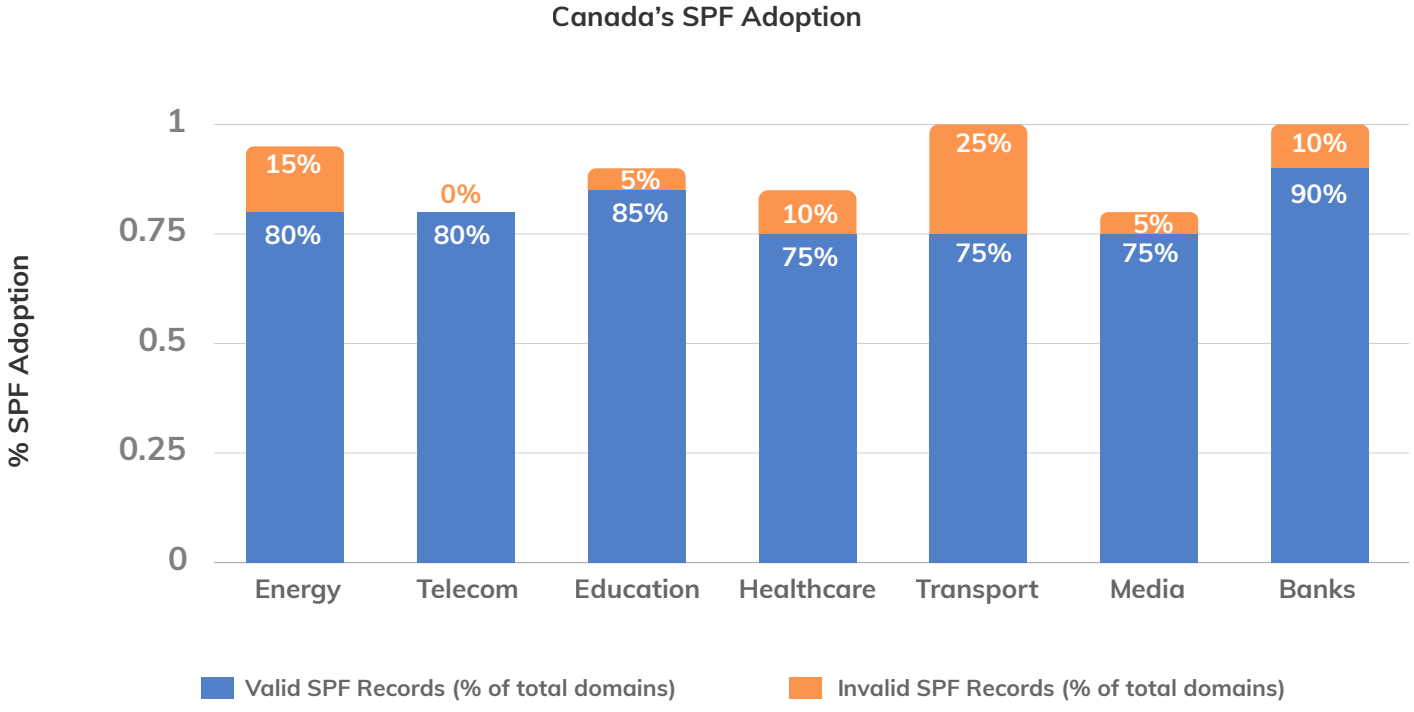
DMARC Adoption Rate in the Canadian Finance Sector



Key Findings:

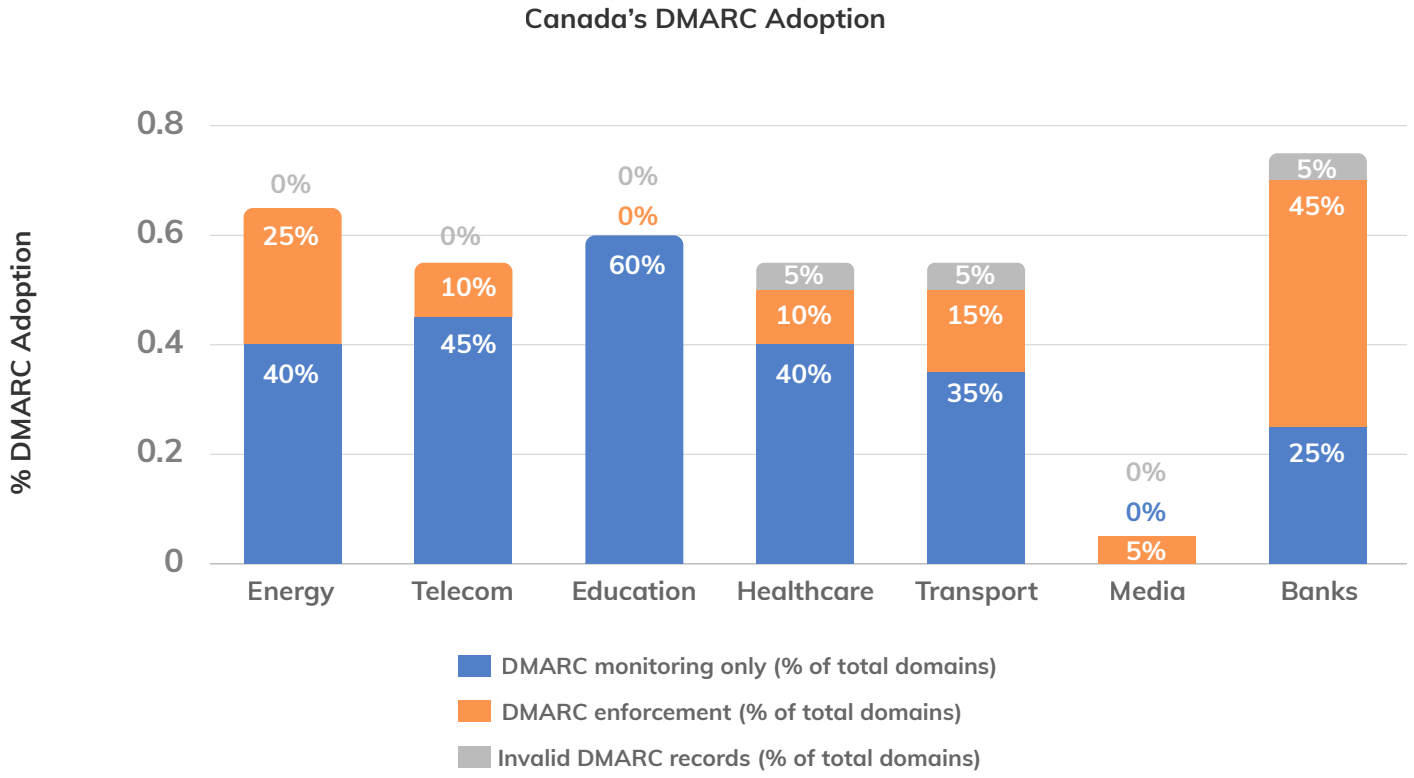
- On a positive note, 90% of the domains in the Canadian banking and finance sector had valid SPF records in place
- However, 25% of the domains contained no DMARC record in their DNS, and a further 25% had their DMARC policy set at monitoring only

Comparative Analysis of SPF Adoption among Different Sectors in Canada



- The SPF adoption rate was found to be the lowest among companies in the transport, healthcare, and media sector in Canada. Canadian banks were recorded to have the highest SPF adoption rate with 90% valid SPF records.

Comparative Analysis of DMARC Adoption among Different Sectors in Canada



- 55% of the banks in Canada out of the total domains analyzed had their DMARC record at monitoring only, the Telecom sector was observed to have the lowest rate of DMARC adoption with only 5% domains at DMARC enforcement. The transport and media sectors also had comparatively low rates of DMARC enforcement. The highest percentage of invalid DMARC records was observed in the Canadian energy sector. This is a low percentage of overall DMARC adoption among organizations in Canada.

Critical Errors Organizations in Canada are Making

On analyzing 140 Canadian domains from various sectors and industries, it is evident that organizations in Canada are making some critical errors that can jeopardize their online reputation and the safety of their clients:

Complete Absence of SPF and DMARC records

Email authentication protocols like SPF and DMARC can help organizations mitigate a diverse collection of impersonation attacks, ransomware, and BEC to reduce the risk of identity thefts and data breaches. The absence of these records among a considerable number of Canadian domains was found.

Presence of Invalid SPF and DMARC records

A surprisingly high number of domains operated by Canadian organizations were misconfigured or had invalid SPF and DMARC records. This meant that email administrators were unable to detect and filter mail from these sources as it was not possible to identify their source. These completely rendered the process of setting up email authentication futile.

Lack of DMARC enforcement

Another prominent finding from the examination of Canadian domains was that while DMARC records existed for a certain percentage of the domains, the rate of DMARC enforcement among them was low, that is the majority of the domains had their DMARC policy set to none, enabling monitoring only.

Note that a DMARC none policy doesn't protect against spoofing, phishing, and ransomware attacks. Only an enforced policy of quarantine/reject can provide a certain level of immunity against impersonation.

Too many DNS lookups for SPF

Since SPF has a 10 DNS lookup limit, exceeding the limit can lead to SPF failure during authentication. One of the reasons for invalid SPF records spotted in the DNS of Canadian domains might be due to too many DNS lookups that can break SPF.

Multiple SPF or DMARC records for the same domain

Among best practices for email authentication, each domain must possess only one SPF or DMARC record for it to be considered valid. The presence of multiple records for the same domain can invalidate all of them.

Steps to be Taken for Improving Email Security in Canada

- One common error made by companies worldwide, including Canada is that after implementing DMARC, they set it to none and expect their domain to be protected against spoofing and business email compromise. The problem is, only a policy of enforcement (p=reject/quarantine) can protect your domain and stop impersonation.

- Other crucial steps to improving the email security posture of Canadian organizations are as follows:

1. staying under the 10 DNS lookup limit for SPF
2. having error-free SPF and DMARC records
3. having a single SPF/DMARC record per domain
4. implementing additional layers of security like BIMI, MTA-STS, and TLS-RPT
5. monitoring your domains and sending sources to pick up on spoofing attempts and email delivery issues

How can PowerDMARC Help You in this Process?

PowerDMARC offers the world's most comprehensive and secure email authentication solutions for companies and organizations of all sizes. Our proprietary DMARC software solution is designed to achieve a secure email ecosystem by combining the power of DMARC, DKIM, and SPF. Companies that implement DMARC in their email marketing solutions reduce spam complaints, internal emails bounces, enhance the deliverability of emails, and stay protected against phishing attacks and ransomware.

- **Configuration:** We take care of configuring your SPF, DKIM and DMARC records.
- **Setup:** As soon as we help you set up your DMARC dashboard, you gain visibility instantly.
- **Monitoring:** We monitor security incidents in email traffic 24X7 and control legitimate sending sources with alerts, reporting, and responsive actions.
- **Reporting:** Daily Aggregate (RUA) and Forensic (RUF) reports help you keep a track on all emails that are passing and failing DMARC from your domains.
- **Enforcement:** We provide full DMARC enforcement (p=reject/quarantine) in record time.
- **PowerSPF:** Allows you to always stay under the 10 DNS lookup limit.
- **Latest Authentication Protocols:** We use the latest email authentication techniques such as MTA-STS and BIMI, along with the standard protocols, to effectively mitigate all impending challenges in email security and authentication.
- **Managed Security Services:** (MSP/MSSP) with a dedicated Service Desk to support your company's DMARC implementation efforts and to monitor the email authentication health of your domain and the safety of your users.

Let's join hands to increase the rate of DMARC adoption and strengthen the email security infrastructure in businesses across Bahrain. Get in touch to find out how we can help protect your domain and business today!