




# SMX DMARC Survey

**Edition 2024**

[smxemail.com](https://smxemail.com)



# Introduction



**Your organisation's cybersecurity may be a fortress, but every email is an open door. Email is still the vector for 90% of successful cyberattacks in Australasia.**

DMARC has been around for almost a decade, with a game-changing approach that identifies and rejects or quarantines malicious or suspicious emails according to the settings of each domain. Yet despite government mandates, the obvious business benefits and calls from industry, organisations have been slow to implement and enforce DMARC. This pace is likely due to a combination of factors. Many businesses may still believe that DMARC only benefits the wider internet community, rather than understanding the tangible positive impact it can have on their own organisations. Plus, more organisations lack the specialist skills needed to enforce DMARC and its dependencies, DKIM and SPF, without disrupting their email workflow.

Organisations have been making progress since our first DMARC survey in 2020. However, deployment is only the first step - **enforcement matters**. DMARC can't protect domains or users while still in report-only mode.

How many Australasian organisations have moved to enforce their DMARC protocols? This year's survey reviews the DMARC status of organisations across six distinct categories:

- NZ government agencies
- The top 100 NZ organisations
- Australian federal government agencies
- SMX's customer base
- Companies listed on the ASX
- Organisations sending email to SMX's customers

# Expert Analysis

**We asked three DMARC and email security experts to weigh in on the numbers and share advice for domain owners.**



**Thom Hooker -**  
**SMX founder, email security expert**

Thom has been at the forefront of email and cybersecurity in New Zealand for over 25 years. Before co-founding SMX, he built his reputation in the early days of the internet with his then-revolutionary approach to the Xtra platform.



**Jamie Callaghan -**  
**SMX head of product**

With more than two decades of experience in cybersecurity, Jamie has designed email security solutions for enterprises, governments and telcos across Australasia.



**Chirag Joshi -**  
**Multi-award-winning CISO**

A multi-award-winning CISO and board member of various advisory boards, Chirag has built his global experience across industries, including financial services, government, energy, healthcare, higher education and consulting.

# Why enforcement matters

DMARC is a revolution in email security. It is a technical standard designed to protect both email senders and recipients from malicious emails. With email still the vector for 90% of successful cyberattacks, properly enforced DMARC should be considered a must-have for any domain owner. When DMARC is implemented and set to enforcement, it delivers widespread benefits.

## Building digital trust, protecting brand and reputation

To engage with or buy from you, your customers need digital trust – should they download your app, make payments or accept cookies?

Malicious emails that spoof your brand can undermine this process. When enforced, DMARC helps prevent these and shows you're serious about protecting users.



**Building digital trust starts early, nearly always with the customer being able to trust your email.**

*– Chirag Joshi*

## Highly effective protection against spoofed emails

Enforced DMARC records contribute to a better-protected internet community by protecting recipients against phishing, whaling and other impersonation fraud. Trusted brands are more likely to be spoofed, so they play a vital role.

Domain owners also benefit from a safer internet ecosystem – your employees can be subject to spoofing attacks (whaling) in the corporate email environment and may also be your customers. Protecting them with DMARC protects your business. “We have seen several instances now where people’s home devices get compromised, resulting in corporate breaches,” says Chirag.



**Prominent Australian and New Zealand brands have an obligation to protect users in their supply chain.**

*– Jamie Callaghan*

## A show of strength

Cyberattackers will look for easy targets. Having DMARC in place and enforced indicates that you’re anything but. “You’re saying to attackers that your organisation takes cybersecurity seriously,” says Thom.

# Why enforcement matters

## Secure supply chain

Some studies suggest that as many as a third of all attacks access corporations through their supply chains. Links to a compromised supplier puts your organisation at risk.

"People trust your providers and partners, which leaves them vulnerable. DMARC in enforcement mode helps protect everyone," adds Chirag.

## DMARC: a key control for holistic cyber risk management

It's easy to think about cybersecurity as a series of technologies and protocols. However, it fundamentally is a risk management exercise. Prudent risk management can only come from taking a holistic approach to controls and DMARC should be considered a key control with this mindset.

The expectation for CISOs today is to take "reasonable and proportionate actions" to mitigate cyber threats, based on threat profiling and organisational context. Implementing DMARC enforcement can provide always-on tracking and protection, delivering real-time insight into threat actors targeting your business's brand and reputation.



**"When people think about email-based threats, they gravitate to filtering, phishing awareness and training, protecting the internal against external threats. At the same time, understanding the risks and sources of spoofing and impersonation are also vital considerations that CISOs need to recognise and address."**

*- Chirag Joshi*

## SECTOR ANALYSIS OVERVIEW

# Google adds weight to government mandates

Even with government mandates and industry best practice advice, organisations have been slow to implement and enforce DMARC.

Late 2023 saw the arrival of DMARC mandates from a source with tangible power: Google.

Since February 2024, new Google mandates have required DMARC deployment from organisations that send over 5,000 daily emails to Gmail accounts.

As of April 2024, Google started rejecting emails from domains without the standard, but it doesn't require enforcement.

This means many businesses are simply deploying DMARC and not moving to enforcement. This serves Google's purpose of better protecting its users, but it means businesses are missing out on broad benefits. These include reducing the risks of phishing attacks, jumping on spoofed domains, and protecting brand reputations.

"Google expects owners to understand how their domains are being abused and then to take action," says Thom Hooker. "But businesses are probably not taking their DMARC reporting seriously or reading those reports."

The mandate is prompting some action, with many of our sector groups increasing deployment numbers.

ASX-listed companies with DMARC in place increased to 59.9% from 29.5% in 2022. Echoing this trend are SMX customers and domains sending to them. This group comprises organisations across sizes, sectors and locations, perhaps showing an overarching picture of our region's progress.

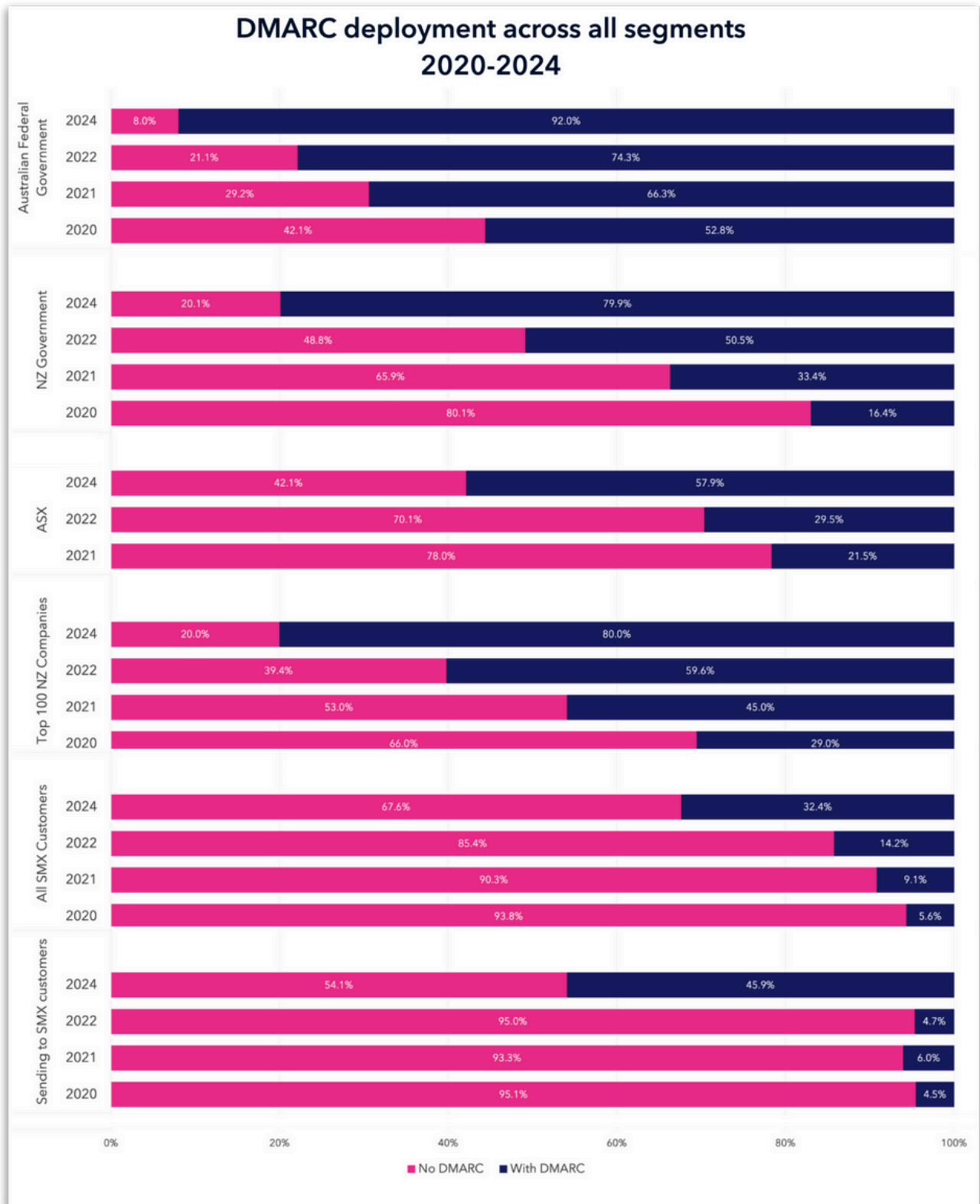
Domains with DMARC records sending to SMX customers is around 45.9% in 2024's survey - a significant increase from just 4.7% in 2022\*. SMX customers themselves also increased deployment over the two years, from 14.2% to 32.4%.

NZ government agencies and the top 100 NZ companies also dropped, halving the numbers without DMARC to 20.0% and 20.1%, respectively.



**Many bulk senders don't appropriately secure and configure their systems, allowing attackers to easily hide in their midst.**

*- Google release, 2023*





# Enforcement still on the to-do list

While Google mandates are driving deployment, the majority of organisations remain unprotected by DMARC enforcement and are missing the business benefits it delivers. Without DMARC enforcement, a domain and its email recipients remain at risk.

**Having DMARC in reporting mode is like fitting a lock on the door but then leaving it wide open.**

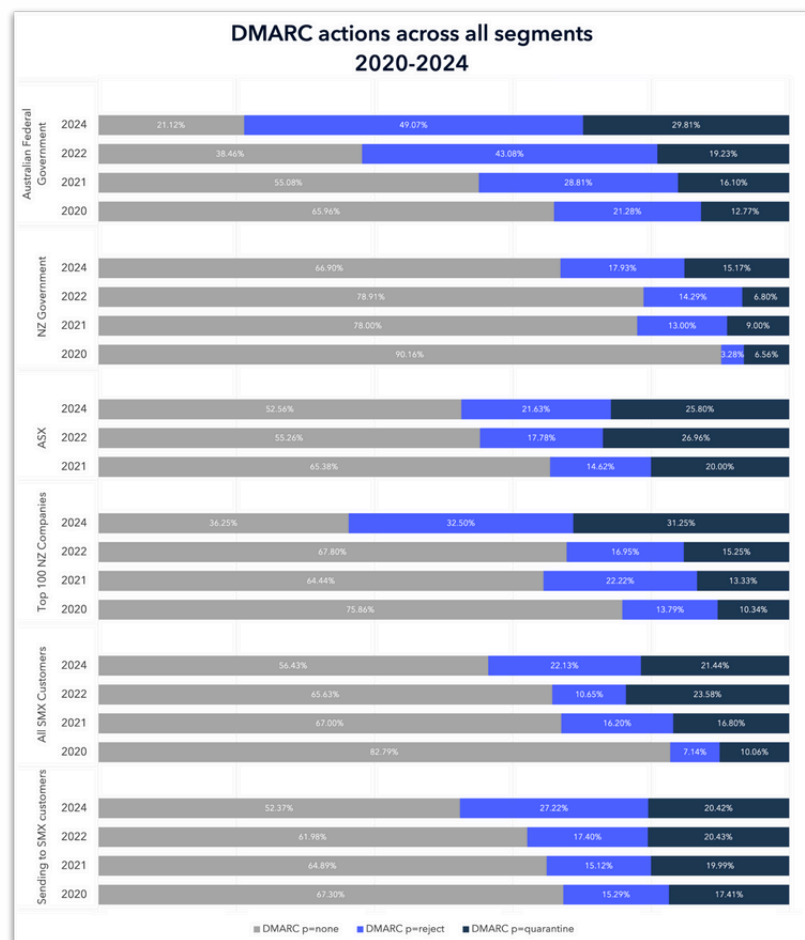
- Nancie Williams, SVP North America, Red Sift

Therefore, the numbers to watch across Australasia are the percentage of DMARC records being properly implemented and enforced. However, if enforcement figures start to improve, some organisations may find themselves at greater risk.

Thom explains that as more organisations deploy DMARC and move to enforcement mode, those left behind will be even more vulnerable to attack. "It's that shrinking pond effect, where you're in a smaller and smaller pool of potential victims."

In New Zealand, government agencies are still generally unprotected, with 66.9% of DMARC records in report-only mode. These numbers are particularly stark compared to only 21.12% of Australian federal government agencies in a similar position.

However, NZ's top 100 companies are setting the benchmark for their Australian counterparts. Of the top 100 NZ companies, only 36.25% have their DMARC record set to report only. In real terms, this still leaves around 50% of these companies unprotected – DMARC is either not deployed or set to report only. The picture is worse for ASX-listed companies. Only 52.56% of those with DMARC records had them set to enforcement mode. In real terms, three-quarters of ASX-listed companies are still unprotected by an enforced DMARC record.



**Three-quarters of ASX-listed companies are unprotected by an enforced DMARC record.**



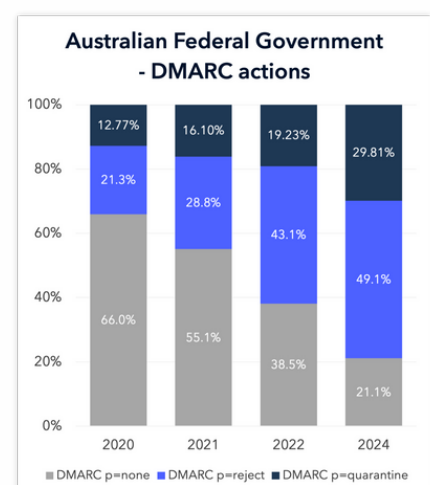
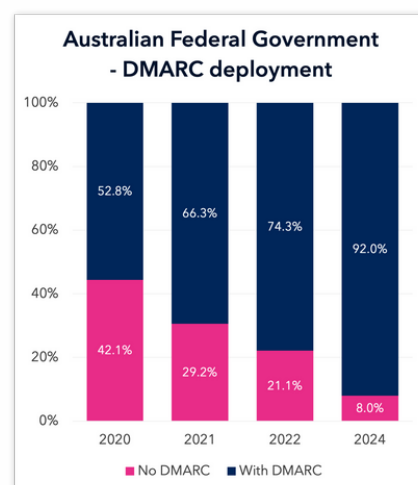
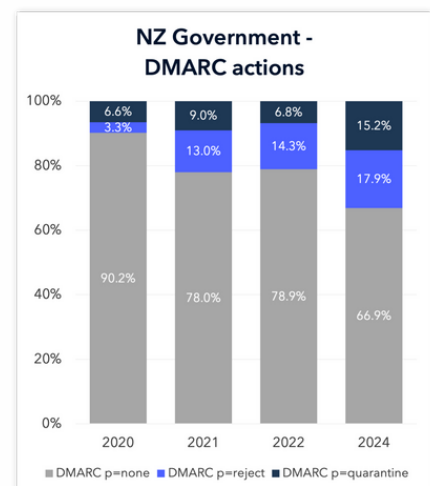
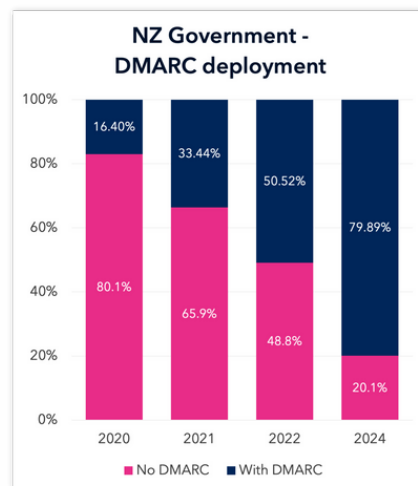
## PER-SECTOR ANALYSIS

# AU government shows the way - NZ lagging behind

New Zealand's Information Security Manual (NZISM) named DMARC a critical part of the protective security requirements for NZ government agencies. Released in September 2022, NZISM V3.6 changed DMARC to a must-do action, which means NZ government agencies have already had nearly two years to conform to the recommendations. Similarly, the NZISM says domains must have moved their records to p=reject for email originating from or received by their domains (see section 15.2.20.C.02). It also includes a recommended approach if a disrupting a domain's emails would impact the organisation (see section: 15.2.16).

Despite this, the sector is only now showing signs of movement. While almost 80% now have DMARC deployed, the majority of those are still leaving agencies unprotected - two-thirds are still in reporting-only mode.

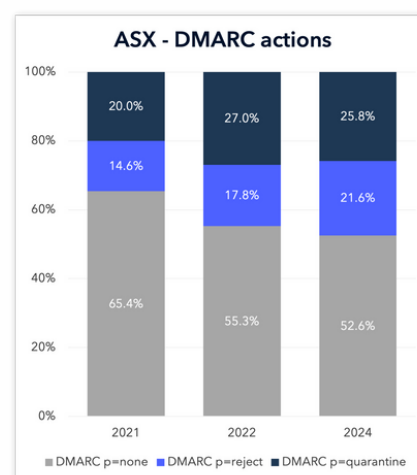
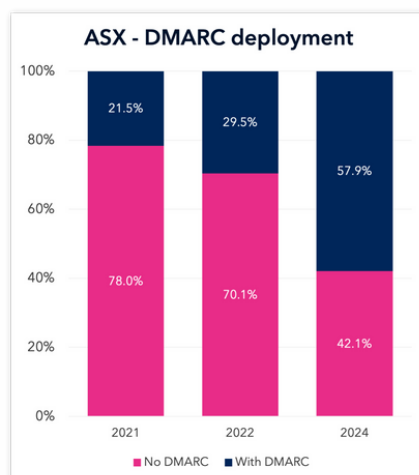
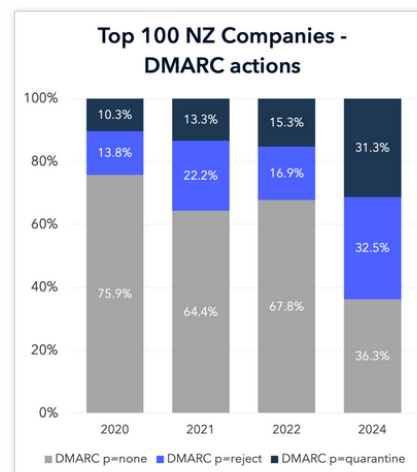
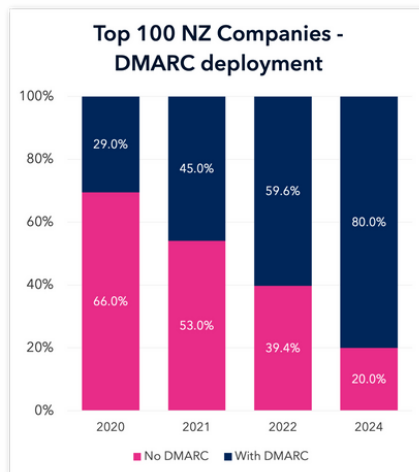
Australian federal government organisations have made the most steady progress towards 100% DMARC deployment and enforcement of all surveyed sectors. 92% of Australian federal government agencies have rolled out DMARC, and 78.9% are in enforcement mode.



# NZ's largest companies a lesson to Australia's

80% of New Zealand's top 100 companies now have DMARC deployed (vs 58% in Australia), and 64% of those with DMARC have it in enforcement mode (vs 47%).

However, there's still more work to do. 100% DMARC deployment and enforcement are essential to protecting more inboxes, companies and people from fraud and attack.

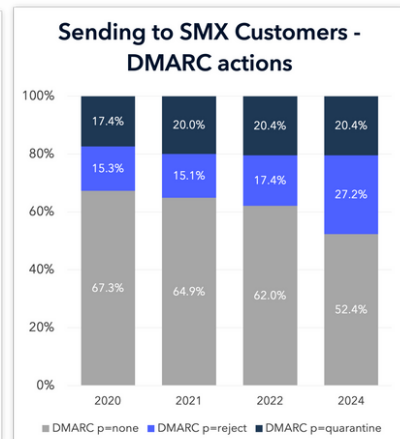
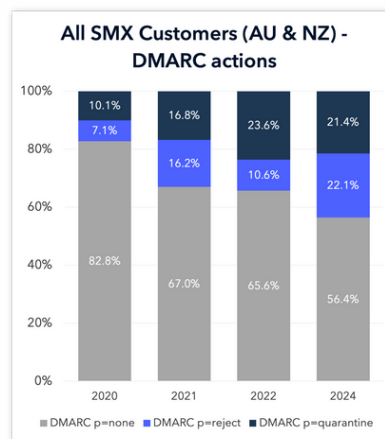
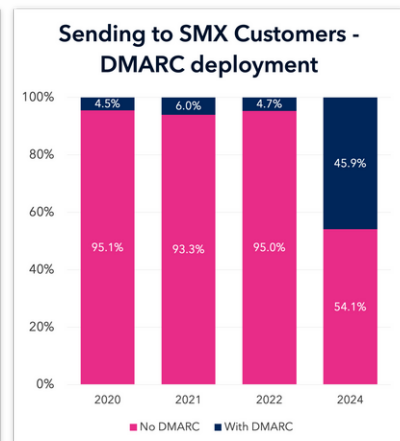
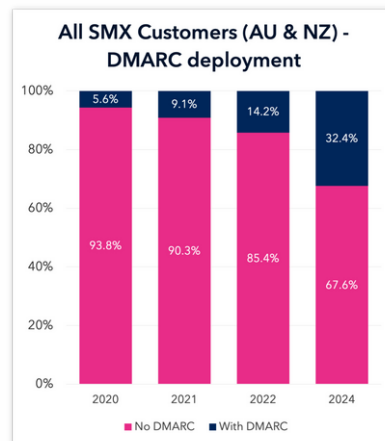


# SMX customers – a market-wide snapshot

While most of our surveyed organisations represent the larger end of the market, we can get a broader snapshot from the DMARC statuses of SMX’s customers and the domains that send to them. We manage over a million inboxes across Australia and New Zealand, which receive emails from multinational conglomerates to sole traders.

Compared with 2022 data, DMARC deployment in SMX customers more than doubled to 32.4%, and deployment in domains sending to SMX customers increased 10-fold to 45.9%.

Enforcement numbers are increasing, too, although more slowly. The percentage of SMX customers in enforcement mode has moved from 34.2% in 2022 to 43.5%, continuing the trend of year-on-year improvements. Still, for both groups, more than half remain without enforced DMARC.



## Small business has a role to play

We expect to see much lower deployment and enforcement numbers in this group – Google’s mandates or other incentives won’t impact many small businesses.

Jamie says that’s a problem, especially for New Zealand, which has a high percentage of small businesses. “90% of New Zealand organisations have fewer than five employees, and some serve high-risk and high-value industries like agriculture,” he explains.

This access makes them attractive targets for attackers looking for a way into client or partner systems. In addition, deploying DMARC can be surprisingly straightforward in a simple environment, and small business owners should talk to their IT support about beginning the process.



## SMX DMARC SURVEY 2024

# Deployment is nothing without enforcement

Year after year, it's pleasing to see more organisations understanding the value of correctly configured DMARC protection – but it's just the start of the job. DMARC can only protect brands and consumers when set to enforcement mode. On average, just over 55% of the surveyed organisations have DMARC deployed and in enforcement mode, leaving 45% unprotected.

That's because many businesses stall after deployment, lacking the specialist skills to ensure configurations won't impact legitimate senders. Email is at the core of every function for most organisations – disruption would be catastrophic, so it's perceived as being simply too risky to move from reporting to enforcement. However, that needn't be the case.

### Enforcement in six weeks

To help clients overcome this barrier, the DMARC experts and SMX designed our Domain Protection Service (DPS). The service combines specialist expertise, a tested process and best-in-class technology to get you to enforcement within six weeks.





# Deep DMARC expertise - SMX

## **Complete risk picture, tailored security**

With our deep expertise, unmatched access to data, cutting-edge pattern recognition and regional knowledge, you get a more complete picture of your external risk. This combination gives you better visibility, control and proactive risk mitigation.

## **Actionable insights, not just information**

Actionable insights, not just information  
Data is only effective if it helps us do better. We turn information into actionable insights so customers can make faster, better-informed decisions.

## **Specialist guides for the digital world**

SMX's virtual security team offers specialised expertise on demand to help you confidently navigate the digital landscape and increasingly sophisticated cyber threats.

**Get to enforcement faster - SMX Domain Protection Service**

[sales@smxemail.com](mailto:sales@smxemail.com)

+64 9 302 0515