



SMX REGIONAL DMARC SURVEY Q1 2021

Released May 2021

By Thom Hooker

Background & Summary findings

In early 2020, SMX carried out the first [Regional DMARC survey](#) to gauge the uptake of DMARC in the Australasian region. We conducted this survey to provide insights for organisations in this region and to provide a comparison for DMARC uptake in other regions.

Our survey analyses data publicly available in the DNS and is designed to highlight DMARC's important role in securing email in the 21st century.

One year on from the initial regional DMARC survey, in April 2021 we again reviewed the DNS in this part of the world to see how the DMARC landscape compares to last year.

The 5 original market segments we looked at in 2020 were NZ central government agencies, their Australian federal counterparts, Top 100 NZ companies, SMX's Australasian customers and the domains our customers correspond with over email.

For the 2021 report we also included the companies listed on the ASX to provide a view of DMARC deployment among large publicly-traded enterprises in Australia.

In summary there has been a big increase in the deployment of DMARC of domains in the Australasian region.

While some of the market segments we monitor have seen relatively modest improvements, some segments, such as the NZ government, more than doubled DMARC penetration from last year. This is great news for users in this region and we're very pleased to see this email security standard starting to get the traction it deserves.

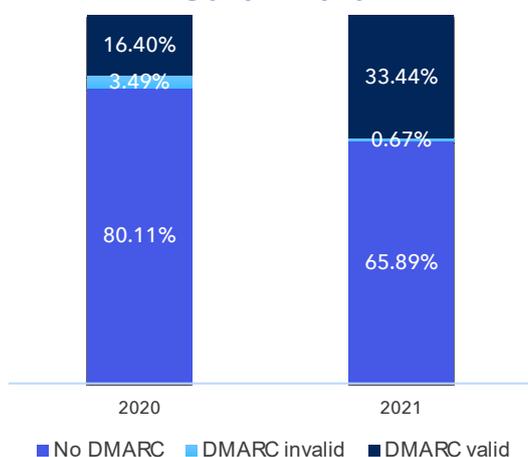
Interestingly no segment we monitor went backwards, which means that even though new domains are being registered the general trend is to deploy DMARC.

"Some segments, such as the NZ Government, more than doubled DMARC penetration from last year."

1. DMARC Deployment by Market Segment

In the following sections we discuss the changes in DMARC deployment over the past 12 months. We report and compare on organisations grouping by those with valid DMARC records, invalid DMARC records or no DMARC at all.

NZ Central Government



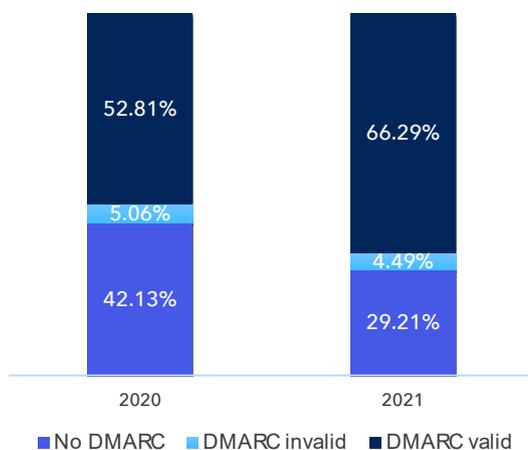
1.1 New Zealand Government

In the NZ Government segment we saw a >100% increase in the number of agencies with valid DMARC records in place compared to 1 year ago. **The percent of agencies with DMARC has increased from 16.4% in 2020 to 33.44% in 2021.** This is a huge increase and we'd like to extend our congratulations to the CIOs and IT teams within the NZ government space - it's fantastic to see more than one third of all agencies now have a valid DMARC record.

Happily we also saw a dramatic reduction in the number of agencies with invalid records over this period too.

However **there are still almost two-thirds of NZ Government agencies with no DMARC at all.** This shows that despite the big gains we've seen in the past year there is still a lot of work to be done in this sector before we can claim 100% DMARC deployment.

Australian Federal Government



1.2 Australian Federal Government

The Australian Federal Government sector already had good DMARC up-take in our 2020 survey, with 52.81% of agencies having deployed DMARC as of last year. **The increase in DMARC deployment over the past year has been almost as large as we saw in New Zealand** with an increase of almost 14% to 66.3%. This is impressive with more than two-thirds of all Australian Federal Agencies now having deployed DMARC.

The bad news is that, as we reported last year, there are a small but significant number of Australian Federal Agencies with invalid DMARC records. Having analysed these records, they are mainly SPF records in the _dmarc.* TXT record which tends to indicate an organisation struggling with their DMARC deployment. Needless to say we've reached out to these organisations to offer our assistance.

Finally, despite the good progress we've seen in the Australian federal government sector almost 30% of agencies still have no DMARC records at all. It'd be great to see if we can close this gap next time Australia!

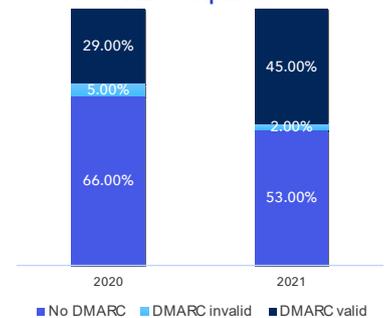
1.3 Top 100 New Zealand Companies

Of all the market segments we monitor this one saw the biggest increase in DMARC deployment over the past 12 months. The top 100 NZ Companies **increased DMARC deployment from 29% to 45%**, an increase of 16 companies.

Happily we also saw a 60% decrease in the number of companies with invalid DMARC records with only two companies now publishing invalid records - well done.

Of course that also means 53 of the top 100 NZ Companies don't have DMARC setup at all and this is a worrying statistic. **Given the size of these organisations and the inherent risks companies of this size attract, this really needs to change with some urgency.**

Top 100 NZ Companies



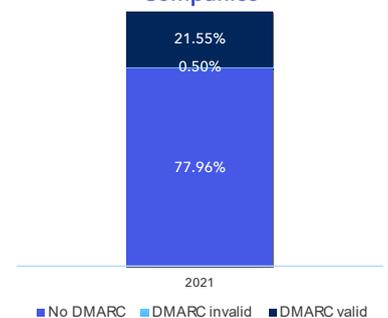
1.4 ASX-listed Companies

While we don't have any data to compare to last year for the ASX-listed Companies we can already see that **DMARC has a reasonable up-take with around 21.6% of companies already having deployed it**, ~390 companies out of around 1800 in total.

And with only 0.5% of ASX-listed companies having invalid DMARC records things aren't looking too bad for this sector.

But with almost 78% of all companies on the ASX having no DMARC at all this is another sector with a considerable amount of work to do in this area.

ASX-listed Companies



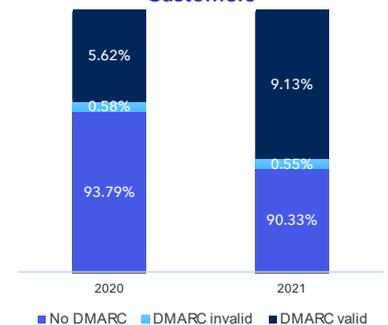
1.5 All SMX Customers

For SMX's customers we've seen a relatively large increase from a pretty low base, with **DMARC deployment increasing from 5.6% in 2020 to 9.1% this year**. While not a huge increase in real terms this is a 62% increase in deployment compared to last year. Well done to everyone who has made the change over the past 12 months.

We also saw a very **modest reduction in the number of agencies with invalid DMARC records**; already the lowest of any market segment we monitor, it is even lower now with just 0.5% of SMX customers having invalid DMARC records.

The disappointing statistic from this segment is that **9 out of 10 SMX customers currently don't have DMARC in place**. This obviously means there's a lot of work to do in this sector and we'll be working with our customers and partners to improve this figure.

All SMX Customers

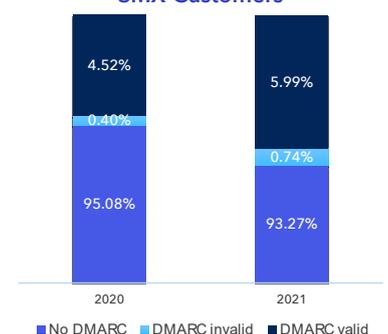


1.6 Domains Sending To SMX Customers

The last segment we looked at in this report was those domains sending to our customers. While the slight increase in DMARC deployment from 4.52% to 5.99% should be acknowledged it shows that progress in this segment is slow.

This segment was also the only one we monitor that reported an increase in domains with invalid DMARC records from 0.4% in 2020 to 0.74% in 2021. **This probably shows that organisations in this segment are wanting to deploy DMARC but are struggling with the implementation details.**

Sending to SMX Customers



2. DMARC Actions

Finally we analysed the actions defined by organisations that have deployed DMARC. In general the trend for companies to migrate to DMARC by taking no action with a $p=none$ setting first is quite evident in the data.

As they become more comfortable with DMARC, these organisations reconfigure their DMARC to take action against emails that breach their policy.

2.1 New Zealand Government

In the New Zealand Government sector we can see a clear progression of agencies from $p=none$ during their initial deployment to $p=reject$ and $p=quarantine$.

In broader terms this sector has matured from <10% taking action on DMARC breaches to 22% now taking action - **more than doubling in 12 months which represent a huge increase**, well done everyone involved here.

2.2 Australian Federal Government

Hats off to the Australian Federal Government Agencies for showing the way, with **45% of all agencies now taking some form of action with DMARC breaches**. While the percentage of Australian Federal Agencies specifying DMARC actions is more than double the number of New Zealand Government Agencies, there are about half the number of agencies in the Australian segment. Either way, there is a big gap opening between the two governments.

2.3 Top 100 New Zealand Companies

In the Top 100 New Zealand company segment we also saw a big increase in the number of organisations configuring their DMARC to take action when breaches occur. This number has increased from ~25% to ~35%, which is great, but it also means that **approximately 65% of Top NZ Companies with DMARC in place are taking no action on emails that breach their policy**.

2.4 ASX-listed Companies

Although this is the first time we've tracked ASX-listed Companies, over a third of them (>34%) have configured DMARC to either reject or quarantine emails that breach their policy. However that still leaves around **two-thirds of ASX-listed Companies that have deployed DMARC taking no action**.

2.5 All SMX Customers

This is another segment that has seen an almost doubling in DMARC actions, from ~17% in 2020 to 33% in 2021. This is great news for the security profile of SMX Customers, well done to everyone involved in this.

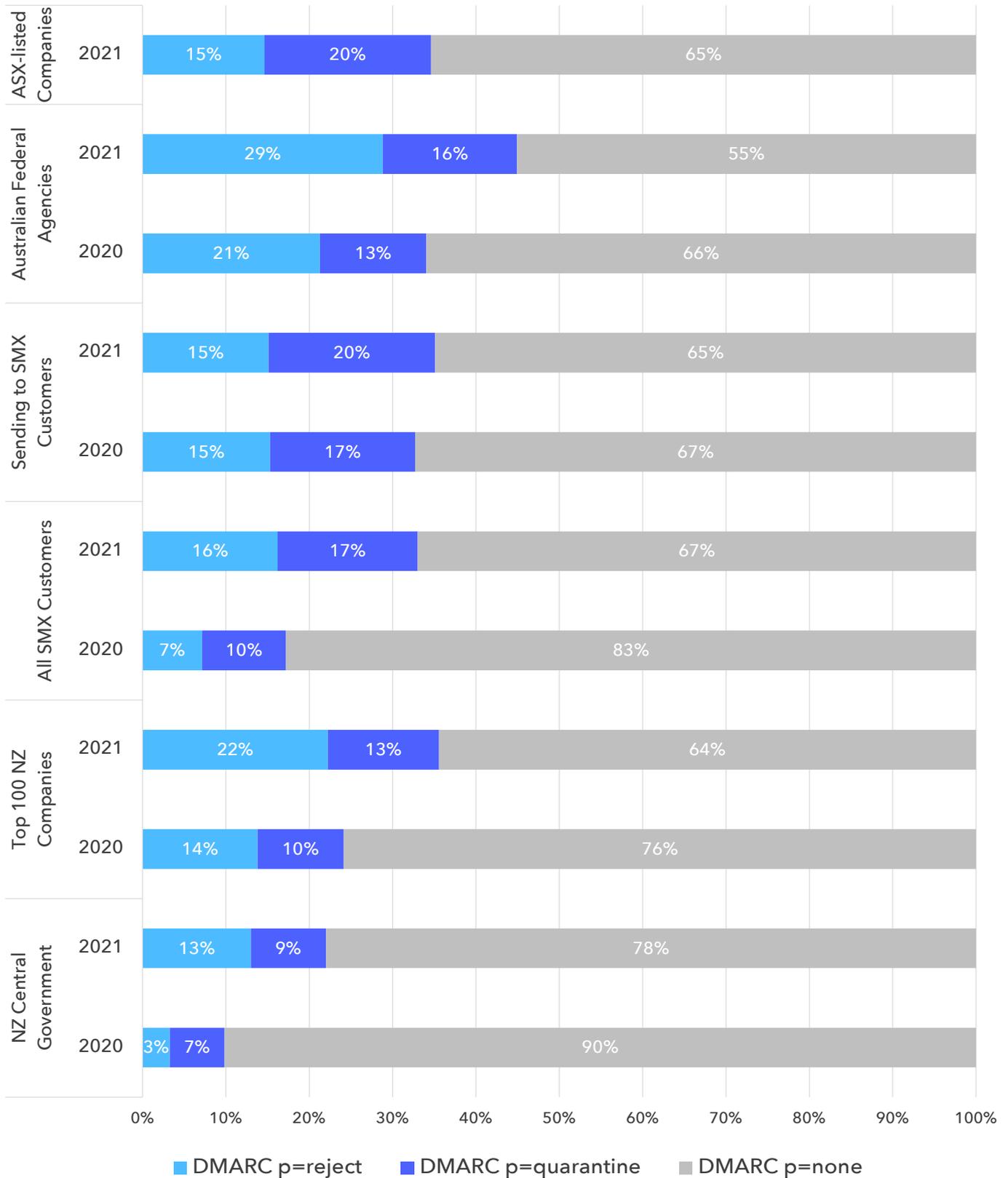
When viewed in conjunction with the big increases in DMARC roll-out among SMX Customers over the past 12 months, this demonstrates a big improvement in DMARC rollout and effective actions being taken against policy breaches.

2.6 Domains Sending To SMX Customers

This market segment saw probably the smallest change in domains specifying DMARC action as opposed to $p=none$ with just a small decrease from 67.3% to 64.9% of domains taking no action.

This led to a **modest increase in domains specifying quarantine ($p=quarantine$) action but we also the only reduction for any segment over the past 12 months**; the percentage of domains specifying reject ($p=reject$) dropping from 15.29% in 2020 to 15.12% in 2021.

DMARC actions across all segments 2020 vs 2021



Conclusion

In summary I would like to pass on our congratulations to all the people and organisations that have enabled DMARC in the past 12 months or who are just starting on their DMARC path now.

There is still a huge amount of work to be done in this space, but we should definitely acknowledge and recognise the achievements to date.

In general, all market segments are slowly increasing their DMARC up-take, some at a faster rate than others.

The evidence is clear: DMARC helps prevent the biggest threats to organisations of all sizes, namely business email compromise (BEC) and email supply chain attacks. Until DMARC is ubiquitous with universal adoption, the risk from these attacks will persist.



The Author: Thom Hooker SMX Co-founder and Email Evangelist

Co-founder of SMX and a Director on the Board, Thom Hooker was previously also the Chief Technology Officer (CTO), responsible for the architecture of SMX's cloud-based email security solution, as well as the hands-on management of product development and customer support.

Prior to founding SMX with Jesse Ball, Thom acquired a wealth of experience and knowledge working for companies including Telecom Xtra, Cable & Wireless, NTL, IBM, EDS, and Air New Zealand. Thom led a development team to design the customised SMX email security solution, built from the ground up as a SaaS platform into which new capabilities and applications could easily be slotted.

With his involvement in architecting large-scale state-of-the-art IT systems, Thom's experience enables SMX to maintain its position as a leader in the messaging and data services market.

About SMX

Over our 15-year history we've seen the transformation to business online, and we know intrinsically the benefits that brings, as well as the risks it opens up.

Over those years, SMX has been part of developing, deploying and supporting email services for enterprise and email providers across Australasia and beyond – and we know that staying ahead of the game takes focus.

Cloud-based email security is our core business, with our points of difference being our focus on localised threats, simplifying migration, rapid adoption of Office 365 email and archiving.

We've also made a name for ourselves in the telco and email service provider world, providing a user-friendly and comprehensive email management service, allowing email providers to deliver and manage full service, fully secure email products to their customers.

- Over one thousand customers with more than one million mailboxes being managed and protected across Australasia.
- Offices in Wellington and Auckland, New Zealand, and Sydney, Australia.
- The largest provider of email security for companies, government departments and organisations in New Zealand.
- A full service business with our own development team creating a number of innovative applications: email archiving tools, custom rules engine, carrier-grade cloud-based email service management.
- Focused globally but supported locally – the scale of service we provide is world-leading, yet we back this with localised, accessible support for solid assistance if needed.

Now, let's talk about making email easy while protecting your people, reputation, and organisation.

CONTACT US

Australia 1800 476 976
New Zealand 0800 769 769
International +64 9 302 0515

sales@smxemail.com
smxemail.com
Connect with us on LinkedIn

