SMX DMARC SURVEY 2022

3rd edition. Released June 2022

by Thom Hooker

Introduction

This is the third year in a row SMX has surveyed the local region (Australia and New Zealand) to measure the uptake of DMARC in this part of the world.

DMARC is the biggest upgrade to email security since the email RFCs were released in August 1982, and our reason for carrying out the annual survey is to raise awareness of this critical email security standard in the local region.

2022 also marks the 40th birthday for email and it's pleasing to see that DMARC is getting some good traction amongst the organisations that stand to benefit the most from its security improvements: enterprises and government agencies that have a large presence in the email world and whose digital assets are relied on by large numbers of people every day.

This year we surveyed six distinct categories of organisations in Australia and New Zealand:

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

Last year (2021), we added the ASX-listed companies for the first time and this year we can compare the changes seen in this group since last year.

Summary

The majority of sectors we surveyed this year have seen big increases from last year's results.

Back in 2020 when we first started this survey, we were disappointed to see how little penetration DMARC had in the NZ government space, with less than 20% of NZ government agencies having deployed DMARC at all. Now, only two years later, the NZ government sector has passed a major milestone with >50% agencies having a valid DMARC record in place.

The NZ government sector showed the biggest increase of any sector we surveyed over the past year, up 17% from last year's result. Pleasingly as well, the percentage of NZ government agencies with an invalid DMARC record has also dropped, from 3.5% in 2020 to <1% in 2022. We would like to pass on a hearty congratulations to all the technical teams within the NZ government space that have worked hard over the past year to understand DMARC and get it deployed on their domains.

While the number of NZ government agencies with DMARC has increased massively in that time, the Australian federal government agencies have been just as industrious. Australian federal government agencies without DMARC in 2020 were sitting around 42% and this has reduced by half in two years to 21% without any DMARC (admittedly there are far fewer federal agencies than NZ government agencies but this is still a huge effort and should be recognised). This means almost 75% of Australian federal agencies now have DMARC in place, 1.5 times the rate of NZ government agencies.

Among the top 100 NZ companies, almost 60% now have a working DMARC record, up from 29% in 2020 and 45% last year. That does mean, however, that almost 40% of NZ's top 100 organisations still don't have DMARC in place.

However, while increasing DMARC uptake by almost 8% over the past year, ASX-listed companies are yet to hit 30% deployment. This means >70% of Australia's largest companies are still without DMARC and are therefore potentially exposed to email spoofing and forgery attacks such as whaling, phishing and payment redirection scams.

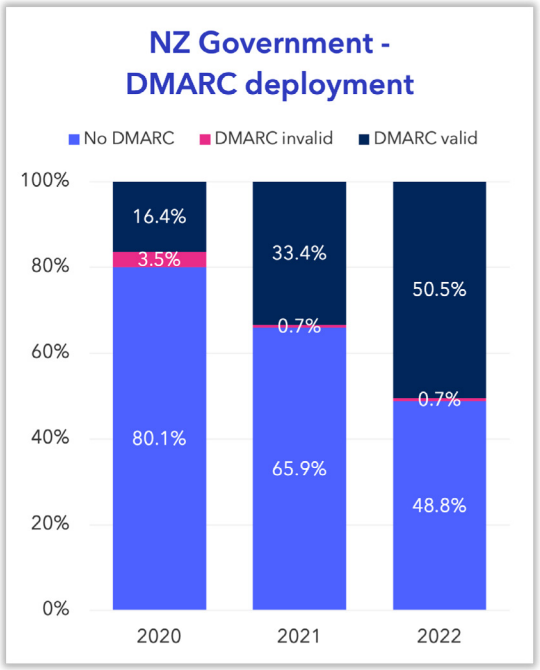
Since our first regional DMARC survey in 2020, we've seen DMARC deployment among SMX's customers increase three-fold, but it was coming off a low base of 5%. Now in 2022, almost 15% of SMX's customers have deployed DMARC, so still a lot of work to do but the trend towards deploying DMARC is clear and happening now (although not as quickly as anyone would like).

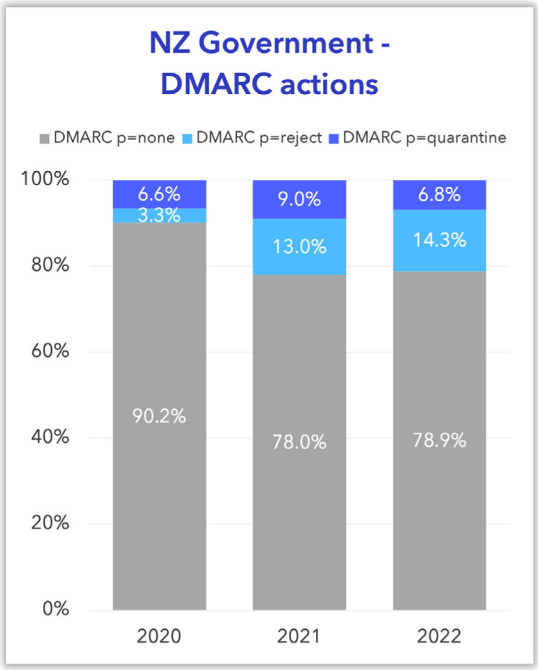
Finally, the only segment that has been fairly static since we began this survey is those organisations communicating with SMX's customers. This segment has been sitting around 5% DMARC deployment since 2020 and hasn't changed much over that time.

Detailed Sector Analysis

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

New Zealand Government





DMARC Deployment

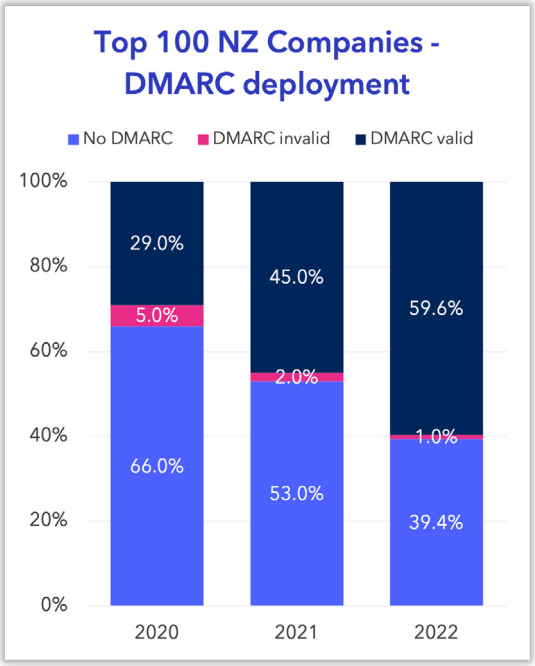
We can see from the data that in a little over two years, DMARC deployment has gone from 16% to just over 50%, more than trebling over those two years. That still leaves about 48% of government agencies without DMARC but we should acknowledge and celebrate this milestone. At the current pace, all NZ government agencies should have DMARC deployed by 2026.

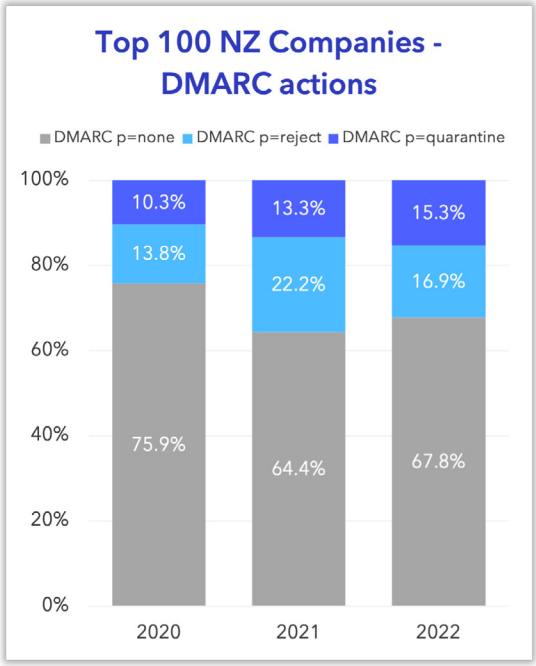
DMARC Actions

This graph shows us how NZ government agencies are choosing to configure their DMARC settings. There has been a significant increase in the number of agencies moving from reporting mode ("p=none") to turning on enforcement mode ("p=quarantine" or "p=reject") which follows the typical pattern of agencies testing DMARC during the deployment phase and then settling into enforcement mode after becoming comfortable that their DMARC configuration is working correctly.
Over the coming years we expect the reporting-only numbers to drop further as more agencies enable enforcement on their domains.

Detailed Sector Analysis

Top 100 NZ Companies





DMARC Deployment

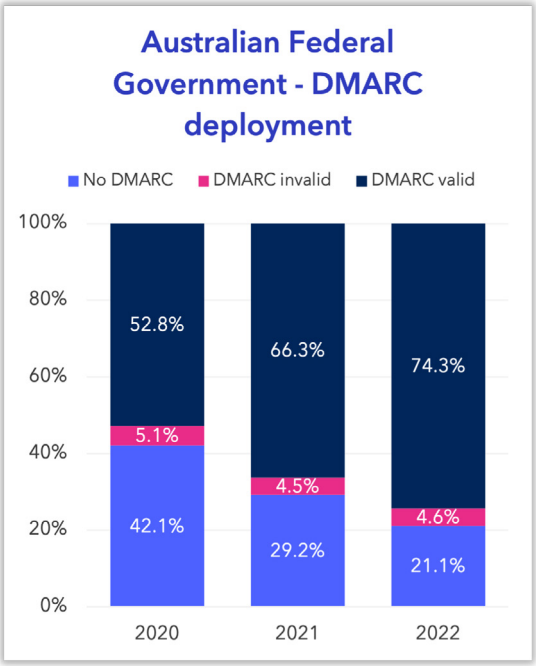
For the largest companies in NZ, almost 60% now have valid DMARC records in place, one of the highest penetration rates of all the sectors we monitor.
This still leaves almost 40% of large enterprises without DMARC.
SMX is pleased to see that the number of large enterprises with an invalid DMARC record has dropped from 5 in 2020 to just 1 in 2022.

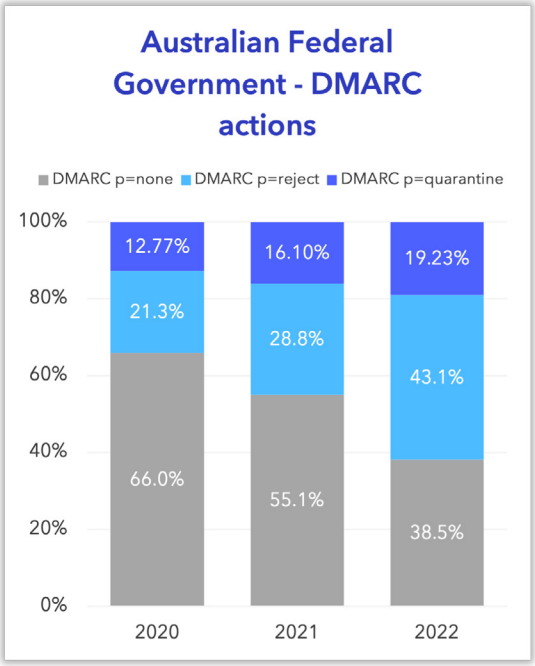
DMARC Actions

While the percentage of companies with DMARC set to reporting only ("p=none") has increased over the past year, and the percentage of companies with enforcement mode of some type has dropped from 35% to 31% over the last year, this is due to the increased number of companies deploying DMARC. This follows the typical pattern of companies deploying DMARC in reporting mode while in the early stages of rolling out DMARC, before moving to enforcement mode after their DMARC settings have had time to take effect and giving them time to update sending sources.
We expect the number of companies with enforcement mode to increase as they become more comfortable that their DMARC configuration is working correctly.

Detailed Sector Analysis

Australian Federal Government





DMARC Deployment

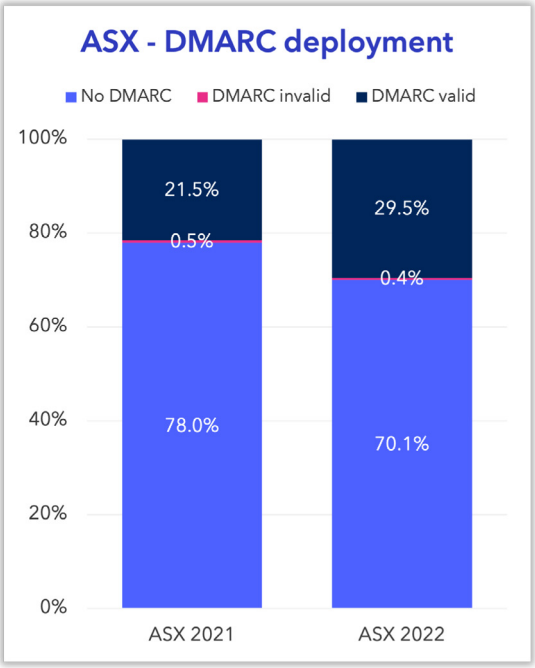
The Australian federal government sector is showing a 50% reduction in the number of agencies without DMARC over the past two years, from 42% without DMARC in 2020 to 21% in 2022 . While there is still a relatively large number of agencies with invalid records, and noting that this number hasn't changed much in the two years we've been running this report (around 5%), almost three quarters of Australian federal agencies now have DMARC in place. This is a huge endorsement of DMARC as government-grade email protection and worthy of deployment by all organisations.

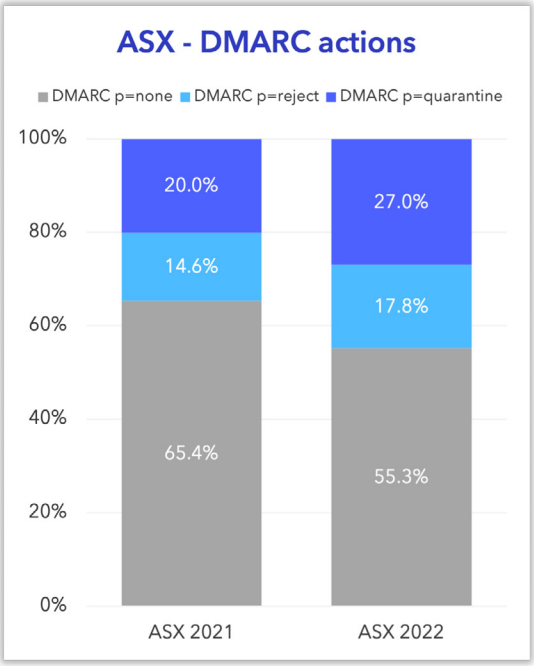
DMARC Actions

The Australian federal government sector is demonstrative of the typical progress made by organisations from initially deploying DMARC in reporting mode through to moving to enforcement mode over time. In this case we can see the number of agencies in reporting mode dropping from 66% in 2020 to 38% in 2022, with the corresponding increases in enforcement mode settings. Interestingly DMARC is held in such high regard by the Australian federal government agencies that the majority of agencies with DMARC enforcement are utilising "p=reject" over "p=quarantine", 43% versus 19% respectively.

Detailed Sector Analysis

ASX-listed Companies





DMARC Deployment

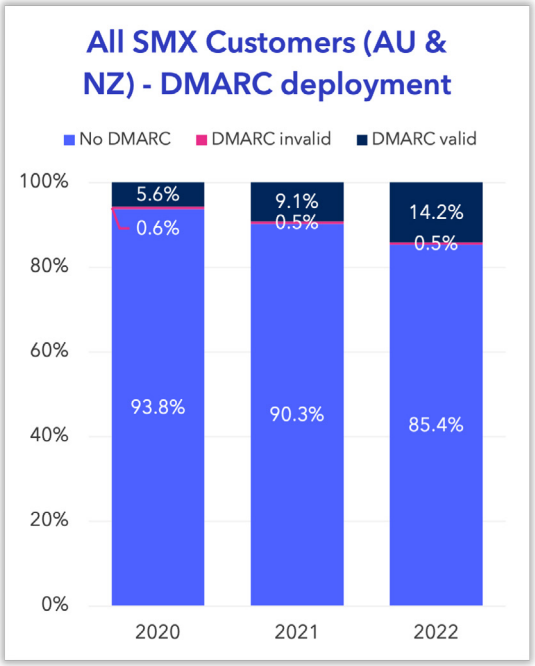
While we've been monitoring the ASX-listed companies sector only since 2021, we can see that there has been progress in deploying DMARC among this group as well. While almost 30% of ASX-listed companies now have DMARC, a huge 70% of them don't have any DMARC at all. These are some of Australia's largest companies and should be leading by example, and taking their customers' security seriously. Still a lot of work to be done in this segment, despite an increase of 8% with DMARC deployed since last year.

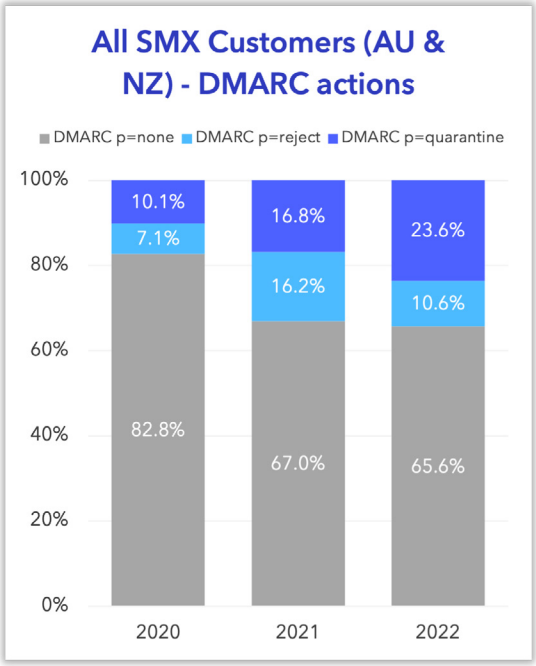
DMARC Actions

Despite the relatively underwhelming/concerning uptake rates among this group, we can see that there has been good progress moving to enforcement mode for those companies with DMARC deployed. With 55% of companies with DMARC deployed in reporting-only mode, down from 65% last year, almost 45% of ASX-listed companies are now using DMARC in enforcement mode – another good endorsement of DMARC among large organisations that carry lots of risk.

Detailed Sector Analysis

All SMX Customers





DMARC Deployment

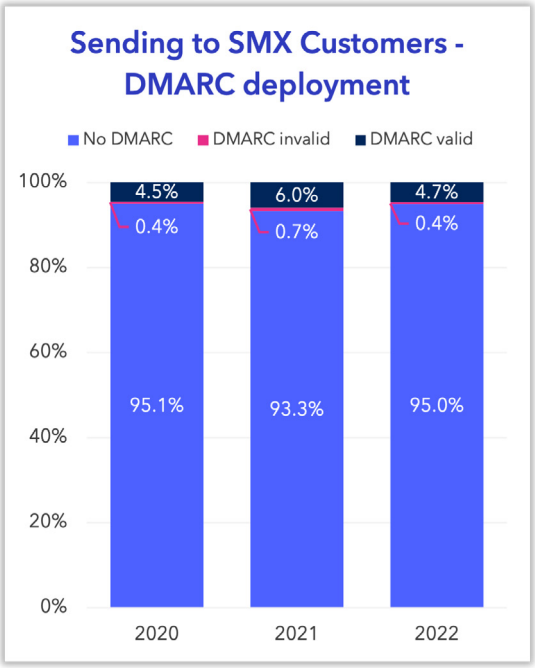
When we first started monitoring the DMARC uptake in the local region back in 2020, our customers were showing very little uptake of DMARC, with just over 5% having deployed DMARC at all.
Now, two years later, this number has tripled to almost 15%.
However, this still means that more than 85% have no DMARC at all, so still a lot of work to be done in this space.

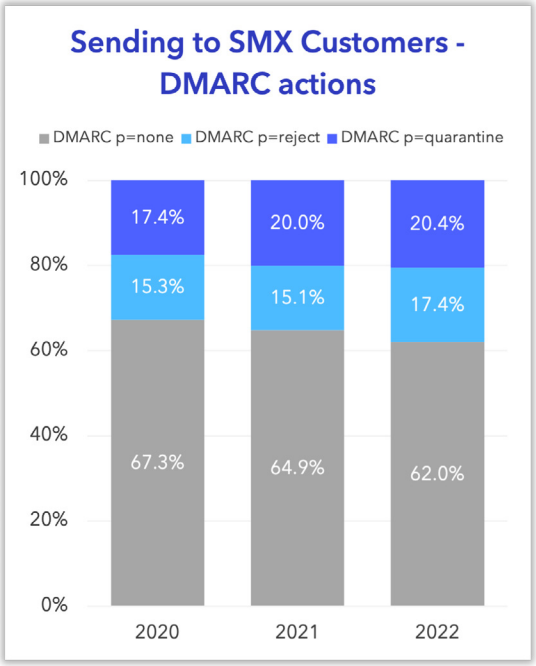
DMARC Actions

Among SMX customers with DMARC deployed we see the typical progression from reporting mode ("p=-none") to enforcement mode. Back in 2020, 82% had reporting mode only and over the past two years this has dropped to <66% with more than 33% of SMX customers now using enforcement mode for DMARC. Well done to everyone involved in getting DMARC deployed and set to enforcement mode.

Detailed Sector Analysis

Domains Sending to SMX Customers





DMARC Deployment

This segment of domains is showing the least movement over the past two years, sitting around 95% without DMARC over that period. While there has been some progress, from 4.2% to 4.7% this segment is showing that many organisations still don't recognise the benefits that DMARC can deliver for themselves and their customers' security.

DMARC Actions

Despite the relatively low levels of DMARC uptake in this segment, for those domains with DMARC deployed we can see the same trends we've seen in other segments with organisations moving to enforcement mode after completing their testing using reporting-only mode. While most organisations in this sector are still using reporting-only mode, an increasing number are using enforcement mode to protect their domains, 37% in 2022 up from 32% in 2020.

Conclusion

Based on the data we've been able to gather for the 2022 edition of SMX's regional DMARC survey, we can see some good progress among all the major segments we monitor. This is pleasing to see as more and more organisations become aware of the benefits that properly configured DMARC can deliver for their domains and digital assets.

Additionally, we can see the trend continuing of domain owners testing the impact of deploying DMARC by rolling out in reporting-only mode, before moving to enforcement mode after confirming their DMARC record isn't causing issues for legitimate senders.

The slow up-take of this revolutionary security protocol is still linked to the perceived complexity of combining a DMARC deployment along with its dependencies, DKIM and SPF.

To help ease the burden of deploying DMARC without negatively impacting an organisation's ability to send or receive email, and acknowledging a skills gap in the current market, SMX has created Domain Protection Service which provides a templated pathway to full DMARC within a defined time-frame. More information on the SMX DPS service is available here.

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 - Email Security Specialists

Cybersecure email. It's all we do.

SMX is a specialist in email security. It's all we do. And that means you access expertise to make your organisation's email a lot safer, for a lot less money than our competitors.

Our in-house development team does that with innovative solutions using email archiving tools, a custom rules engine and carrier-grade email service management.

Here's what you'll get with us

Proven systems

For more than 17 years, SMX has developed, deployed and supported email services for enterprises and email providers in Australasia and beyond.

Local focus to stop local threats

We have offices in Auckland and Sydney, so our world-leading service is backed by an understanding of Australasia's unique threat landscape.

Simplified migration

Getting you onto the cloud is the first step to shoring up your email.
By simplifying migration, we enable rapid adoption of Microsoft 365 email and archiving.

Virtual teams of email security experts

Our team helps you sidestep the reputational damage and financial impacts of email security breaches. You'll prevent Day Zero Attacks and immediately improve your cybersecurity profile.

Protect your email, protect your brand.

TALK TO US

Australia	1800 476 976	sales@smxmeail.com
New Zealand	0800 769 769	smxemail.com
International	+64 9 302 0515	Connect with us on **LinkedIn**