macquarie
CLOUD SERVICES

Zero Trust in Action.

Practical Steps to radically improving your security posture.

By Naran McClung
Head of Azure and Consulting
@ Macquarie Cloud Services

1800 004 943
macquariecloudservices.com

Introduction.

Cyber attacks and data breaches have been in the news - and the issue isn't going away. While these attacks aren't new, there are several factors that have upped the stakes recently:

Data is everywhere, and people want to access it anywhere, at any time.

There has been a massive increase in demand for cloud and Software as a Service (SaaS) services:

The shift to remote work during the pandemic has expanded the attack surface, while also shifting the network load to the perimeterless internet.

Only **25%** of Australian businesses are insured against cyberattacks

Source: *The Conversation – Just 25% of businesses are insured against cyber attacks. Here's why.*

macquarie CLOUD SERVICES

Last year the Australian Cyber Security Centre received 76,000 cyber-crime reports – up 13 percent on the previous year. Cybercrime cost the Australian economy an eye-watering $42 billion in 2021.

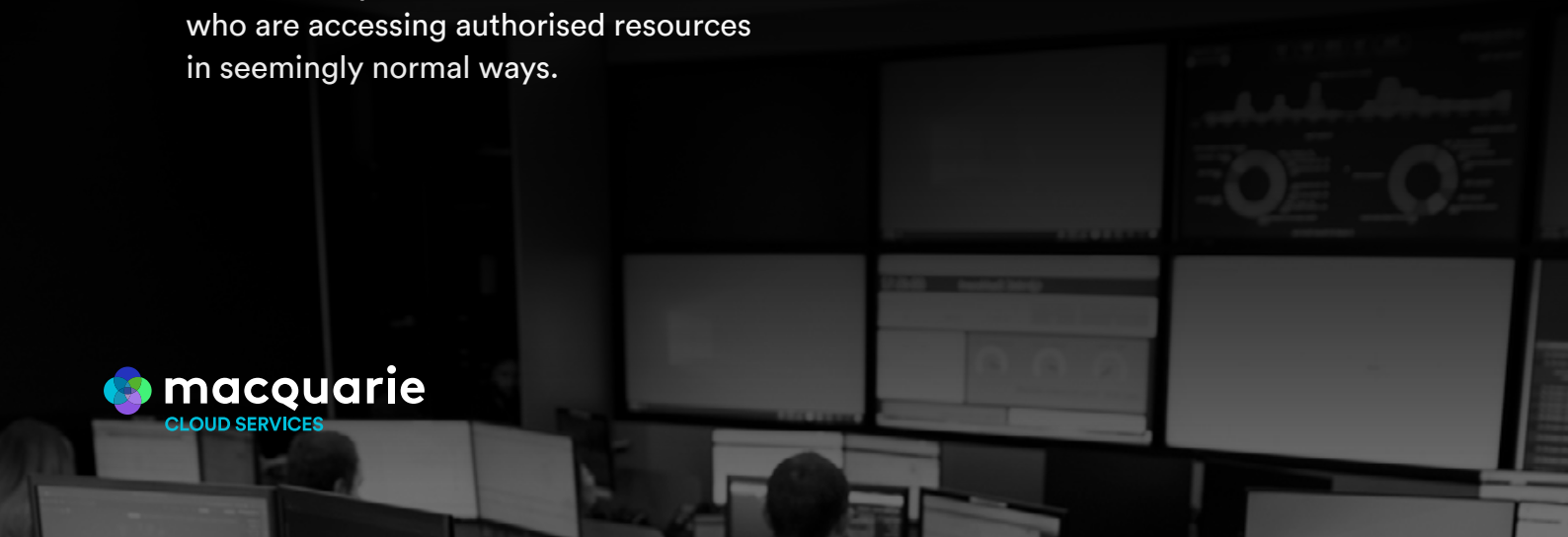
And yet, many companies seem to be drastically underprepared for an attack. Many are lucky to have a basic cybersecurity response plan in place, let alone comprehensive risk management measures such as cyber insurance.

Why should we move on from old cybersecurity strategies?

Put simply: it's time to move on because they no longer work:

- IT environments are far more complex than they were a few years ago, with the rise of hybrid/remote working and continued adoption of cloud technologies.
- Cyber threats are increasing in number and sophistication, and are harder than ever to anticipate and prepare for. Many of the cyber events we see today don't raise concern in the early stages, because they involve authorised users who are accessing authorised resources in seemingly normal ways.
- Many people think that cybersecurity tools are expensive and difficult to use,and offer poor return-on-investment.
- We are experiencing a significant shortage of tech skills across the economy, and companies are fighting it out to hire the right people to deliver cybersecurity capabilities in-house.
- Affordable cyber insurance is a mythical beast for many companies, because they struggle to meet provider expectations around environment security. This also overlaps with demonstrating compliance to the industry regulator.

Enter Zero Trust: the new 'best practice' approach to security management, where regardless of your controls and your investments, you must always assume they're inadequate.



What non-technical leaders need to know about Zero Trust.

Zero Trust is so different from previous approaches to cybersecurity because it assumes by default that a breach will happen - no matter how effective your controls, visibility and perimeter security appear to be. You must assume the worst and continually mitigate against all the possible outcomes.

As with existing cybersecurity approaches, threat detection and response is a critical component of Zero Trust. However, it also calls for deeper strategic thinking - and this is where non-technical leaders add value.

A Zero Trust mindset starts at the executive table, with leaders coming together to develop a shared and comprehensive understanding of the ramifications of a breach. This discussion should extend far beyond the technical implications. What does the worst case scenario look like in terms of loss of data (both personal data and company intellectual property), as well as financial consequences and reputational damage?

This shared understanding of risk is critical. It will minimise the leverage an attacker has on your business in the event of an attack – and again, where you're assuming breach can happen.

Ask your tech team two questions to find out if Zero Trust is right for you.

1 Have we defined the resources we need to protect, their location, as well as the typical activity we should see around them?

2 Are you confident that every user, application (both managed and unmanaged) and device is secured, in every interaction with our environment and shared services?

If the answer to either question is "no" or "I'm not sure", it's time to consider a move to Zero Trust. You could be exposing yourself to substantial risk.

macquarie CLOUD SERVICES

The technical stuff.

Zero Trust is about replacing implicit trust with explicit trust. This means continually assessing and adapting as necessary by evaluating identity and the context surrounding the interaction with your environment. Only then can you determine what level of access is appropriate.

It's just as important to understand what Zero Trust is not:

Zero Trust is not a single product. It is an approach incorporating many layers and decisions that work together to minimise the attack surface.

Security products should support the Zero Trust approach for your organisation, but any product promising to deliver Zero Trust should be regarded with suspicion.

Zero Trust is not based solely on identity. Though an important component of an overall strategy, there are four critical components of an effective approach to Zero Trust: identity, context, resources and control.

An effective Zero Trust approach also takes into consideration user activity, location and time for a more complete view of overall behavior and intent, as well as application instance awareness that may require identity revalidation.

Zero Trust is not a short-term solution that can be deployed in minutes. The journey to a more mature and secure state via Zero Trust is ongoing. It requires both short- and long-term strategic planning and investment.

What are the actual benefits of Zero Trust?

It's hard to argue with Zero Trust as a theory. However, it can also solve the real-world challenges that are top of the agenda for most IT leaders, which include:

Enhanced visibility over cloud service and web use

Secure managed cloud services such as Microsoft Azure, Office 365 and Dynamics 365

Safely and selectively enable unmanaged cloud services, rather than block them all

Identify and control 'Shadow IT' applications within your environment

Have the same level of protection right across the managed environment, regardless of location, device in use or resource being accessed.

However, the benefits go further than that. Zero Trust principles also happen to align almost seamlessly with the expectations of most cyber insurance providers when it comes to environmental maturity. There are no guarantees – but it does mean you'll be in a better position to negotiate affordable coverage or gain coverage at all.

Don’t go it alone, partner wisely.

Zero Trust is a broad set of principles and approaches, so it’s not always realistic to build and execute a Zero Trust strategy in-house. Instead, you can progressively build out a more simplified pathway to Zero Trust architecture by deploying an expertly designed Azure Landing Zone combined with the visibility of Managed Detection Response (MDR). With Microsoft being the only hyperscaler that’s also a security provider, MDR powered by Microsoft Sentinel is a logical place to begin.

MDR is a longer-term partnership with a specialist managed service provider that matches advanced threat detection, incident response and security reporting to the business context. Your partner should arm you with security insights specific to your business. In the event of an incident, you will be working with a team familiar with your infrastructure and operations.

Perhaps most significantly, an MDR partnership should assume shared responsibility and shared risk. The stakes are high for everyone, so your partner has just as much to lose from a reputational perspective in the event of a newsworthy, catastrophic breach.

Make sure your partner knows, understands and is prepared to help you navigate the risks together.

Choose wisely: Questions to ask MDR partners.

Before selecting an MDR partner, ask the following questions:

- [ ] Are they a specialist Microsoft security provider, and recognised as an Azure Expert MSP? This is critical no matter what security products you have in place, as the vast majority of people consume Microsoft services in some shape or form. Improving your Microsoft security posture will go a long way towards improving the security of your environment as a whole.
- [ ] Are they a member of the Microsoft Intelligence Security Association (MISA)? MISA brings together the top experts from across the cybersecurity industry with the shared goal of improving customer security, so you know your partner has access to the latest and greatest thinking.
- [ ] Does the service offer a 24X7 team of onshore security experts with deep cybersecurity experience, coupled with industry leading SIEM/XDR technology?
- [ ] Do they offer advanced threat intelligence feeds and management in real-time, to help you understand and interpret threat intelligence data from various sources?
- [ ] Do they understand the regulatory environment of your business, and can they help with compliance?
- [ ] Can they provide custom analytics and high-level dashboards for reporting at the executive and board level, as well as in-depth technical and operational reports?

Start your Zero Trust journey with a single step.

Macquarie Cloud Services is the leading Microsoft Security Specialist. We are the only Microsoft partner in Australia to be both an Azure Expert MSP and member of MISA.

Our 30-day MDR Proof of Value engagement allows you to immediately bolster your security capability and take the first steps on your Zero Trust journey with a 24 X 7 team of onshore security experts famous for their world class customer service. You'll benefit from tangible security outcomes including out 20+ years of deep security expertise securing Australian government, and enhanced visibility of your security posture right across the business.

Contact us on **1800 004 943** or email us at **enquiries@macquariecloudservices.com** to set up a Proof of Value and kick off your Zero Trust journey today.

macquarie CLOUD SERVICES

macquarie
CLOUD SERVICES

1800 004 943
macquariecloudservices.com