CASE STUDY

How RED21 Grew Into a Security First MSP

RED21 are a long-standing MSP based in Australia with a reputation for being capable and deeply committed to the people they support. They work with a broad range of clients, from family offices to highly regulated financial services firms, and offer their clients no-fuss expertise and excellent quality of service.

For years, that meant focusing on the traditional MSP work that so many of us know well: helping companies with their day to day challenges, keeping their systems running and making sure everyone could get on with their jobs without too much drama. They were the sort of partner who felt more like an internal IT department than an external provider.

Over the last few years cybersecurity has moved from the edges of the industry into the centre of it, and it did so very quickly. Clients began receiving cyber insurance questionnaires. Regulators raised expectations. The Australian government updated privacy legislation. Essential Eight became something organisations could no longer avoid. It was a lot, and it came all at once. Quickly, RED21 realised they needed to adapt cybersecurity into their offering.



“We were very solid on the traditional MSP side of things, but not cyber aware in the way the industry suddenly expected. Clients, insurers,

auditors, the government, everyone started asking for things at the same time."

Tim Canning, Director, RED21

Transitioning to a Security-Focused MSP

For many MSPs, the natural answer would have been outsourcing. Hand the security work over to an MSSP and continue focusing on what they already knew well. But that approach did not align with how RED21 operate. They sit tightly alongside their clients. Passing security to a distant third party simply did not match the culture they had built.

Instead, they made the decision to grow into a security led-MSP. Not loudly or dramatically, but quietly and deliberately. They wanted to create a baseline level of protection for all their clients and make cyber security part of their everyday service, not an optional extra.

It was a significant shift, and one that required new tooling, new thinking and a new kind of confidence. They already had Microsoft Business Premium as a foundation, but as Tim described, Microsoft leaves a lot of the heavy lifting to the MSP. Logs, alerts, recommendations, secure score improvements. All essential, but all demanding time and expertise.

"We needed something that helped us move forward without hiring a whole cyber team overnight."

Tim Canning, RED21

Where RoboShadow Fits In

RoboShadow appeared at an early point in their transition through a recommendation from a sister brand, and it became one of the first tools that helped RED21 feel they could step meaningfully into the security space without becoming overwhelmed.

“It gave us something we could actually use straight away. Somewhere to start, without it becoming too much."

What helped most was how approachable it felt. It did not require layers of specialist training or a dedicated team to interpret the results. It gave them visibility, structure and clarity. They could see vulnerabilities across every client quickly. They could start producing reports for boards and insurers. They could begin having security conversations backed by real information.

A few things stood out for them early on :

- Multi tenant visibility that did not need extra configuration
- Clear vulnerability assessments they could act on immediately
- Time saved by not having to piece together information from multiple sources
- Straightforward reporting for clients and auditors

The Ubiquitous Rollout

Once RED21 had the right foundations, they made an important decision. Security would not be optional. It would be part of their service for all clients, regardless of size.

Many clients understood immediately. Others took a little longer, but as cyber incidents hit the news more often and as compliance requirements spread across sectors, even the hesitant ones began to see that security was not optional anymore.

RoboShadow became one part of a broader set of tools that RED21 now use to look after their clients comprehensively. They added ThreatLocker for application control and a managed SOC. They standardised on Cloudflare Zero Trust as the SASE platform across all clients. They implemented user awareness training through Breach Secure Now.

Together, these tools created the baseline they were aiming for.

A client working with RED21 now gets:

- Up to date devices with strong configuration
- Controlled applications and no unexpected software running
- Users who are trained and refreshed regularly
- Clear visibility of risks through ongoing vulnerability scanning

- Reports they can use for auditors, boards or insurers
- The comfort of knowing someone is watching the security landscape on their behalf

"If you work with us, you are secure. Your users are trained. Your applications are controlled. Your systems are up to date. And you do not have to think about it."

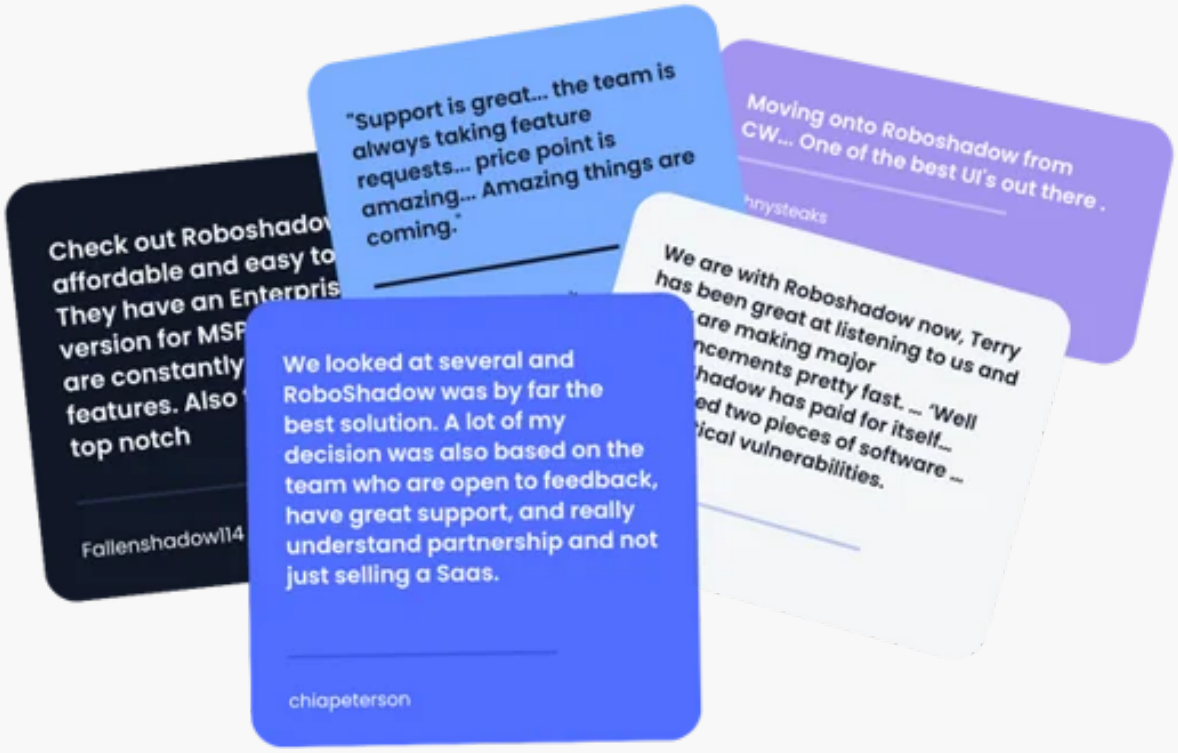
The RoboShadow MSP Advantage

When asked what the biggest change had been for RED21, Tim did not jump straight to revenue or margins. He talked about time, risk and that feeling MSPs know all too well: **the 3am worry.**

As an MSP backed company themselves, RoboShadow helped them reduce those moments. It helped them feel in control of the work rather than buried under it. And it contributed to a more confident, structured security practice that they can continue building on year after year.

Security has also allowed RED21 to reshape their client relationships. Instead of being pulled into cyber work reactively or under pressure, they can now guide those conversations calmly and proactively. It has strengthened trust rather than strained it.

There have been financial benefits as well: as RED21 improved their offering, they were able to package their service properly, supply their own tools and move away from letting clients dictate mismatched technologies. It has made their operations smoother and their service more consistent.



Looking Ahead

RED21's journey into becoming a security focused MSP has not been about a dramatic reinvention. It has been about steady improvements and implementing the right toolsets and workflows.

With RoboShadow now part of their ongoing process, the team can look ahead with confidence rather than pressure. They have the space to fine tune their stack, deepen their automation and bring more consistency to every client they support. Most importantly, they have created an environment where cybersecurity is not something added on, but something woven naturally into the way they work.