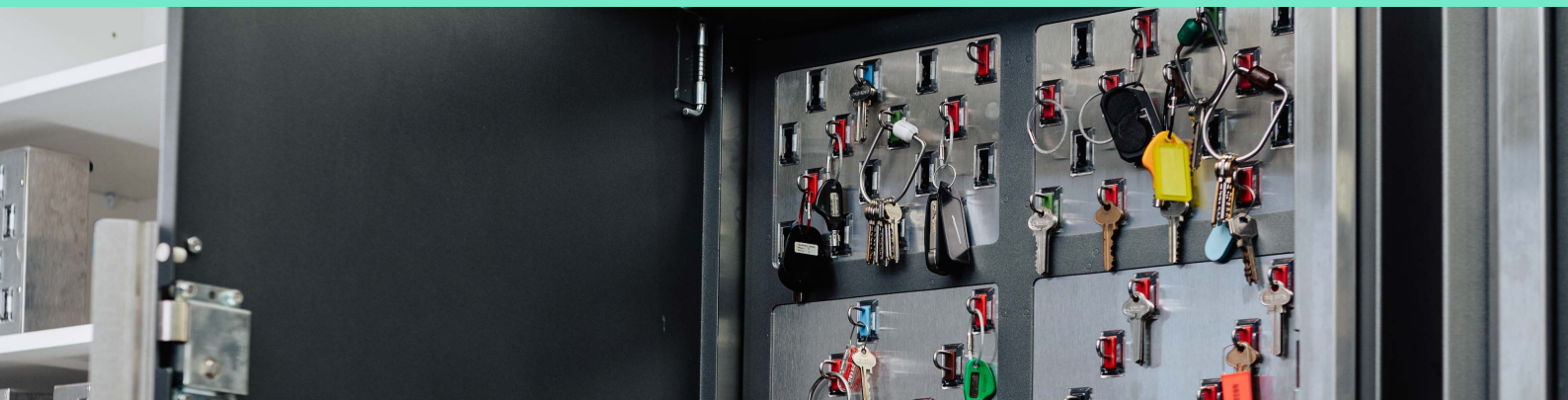


Unlocking failproof connectivity in the face of national outages

How KeyWatcher Australia partnered with M2M One to safeguard critical access for its customers with Fully-Managed Failover.



Keeping staff safe, ensuring assets are protected, and managing secure access to buildings and facilities is a challenge faced by hundreds of Australian businesses. It requires a complex mix of hardware and digital infrastructure. For organisations with large or remote sites, the risk of network outages or unreliable technology carries significant risk. In the worst cases, this can lead to financial or even human loss.

Key management is a critical practice for these businesses to secure assets, approve access, and ensure the health and safety of staff and visitors. But as these systems become increasingly connected, and reliant on major telecommunication networks, new challenges are emerging.

Recent network outages in Australia have underlined the importance of delivering reliable connectivity. Telstra's July outage had widespread repercussions – disrupting payment systems, public transport and even electric vehicle charging nationally.

Such outages have led organisations like KeyWatcher Australia to strengthen connectivity for their customers and protect them from unforeseen network disruption by deploying M2M One's Fully-Managed Failover Service.

A history of innovation in access security

Founded in the 1990s, KeyWatcher Australia began as Australian Security Technology (AST); Australia's official distributor of the Morse KeyWatcher cabinets. Recently, that hardware heritage has evolved into a fully connected digital platform. KeyWatcher Australia's cloud service, known as KeyMaaS, automates key tracking and logging and integrates into security and facility management systems – creating a seamless, connected solution for areas including contractor management, health and safety compliance, and building access control.

Today, KeyMaaS operates across 600 plus sites in Australia, New Zealand and the USA. Customers include hospitals, universities, financial institutions, government facilities and large retail and corporate campuses. More information:

keywatcher.com.au/key-management-software



The KeyWatcher Touch — intelligent key management, connected through KeyMaaS.

The challenge: when the network goes down, so does security

For KeyWatcher Australia, the risk of a national outage was direct and tangible. Its KeyMaaS system relies on constant connectivity. Losing that connection creates significant exposure with a single lost or inaccessible key costing up to \$100,000 to replace. Network downtime also raises the risk of theft and health and safety breaches.

Having operated solely on Telstra's network for approximately five years, KeyWatcher Australia began receiving reports from customers in regional areas of patchy, unreliable signals. The issue came to a head when a university reported dropouts across 45 KeyWatcher units. This led to poor visibility of key and card status during downtime — directly impacting the security and safety of staff, students and campus facilities.

\$100k

potential cost of a single lost or inaccessible key

45 units

hit by dropouts at one university campus

600+

sites running KeyMaaS across AU, NZ and the USA

100%

of connectivity issues eliminated since rollout

The solution: a fully managed dual failover network

To resolve the issue, and protect its customers from future outages, KeyWatcher Australia partnered with M2M One – building on its existing relationship. M2M One designed a dual failover solution that paired native Optus SIMs with KeyWatcher Australia's existing Telstra SIMs. This was backed by dedicated VPN services and continuous data monitoring.

M2M One solution:

- Primary Telstra SIM paired with native Optus SIM
- 24/7 network and data monitoring
- VPN services
- Personal account management.

The rollout for KeyWatcher Australia's university customer was completed in Q4 2025. It has since eliminated all network connectivity issues, whether caused by patchy regional signal or major nationwide events like the Telstra outage.

The outcome: a platform built for growth

Having proven the effectiveness of M2M One's failover service, KeyWatcher Australia is looking to make it their default solution and roll it out to customers across Australia and New Zealand – with USA also on the horizon.

"The recent outage demonstrated the value of M2M One's dual-carrier service offerings. In the past, an outage of this scale would have disrupted contractor and vehicle access for our customers. The outage provided real-world validation that our investment in carrier redundancy was worthwhile, delivering the resilience and business continuity we had planned for."



LIAM BENNETT · IT DIRECTOR, KEYWATCHER AUSTRALIA

What made M2M One KeyWatcher Australia's first choice

- ✓ Low-latency native SIMs
- ✓ Personalised in-country account management
- ✓ Speed of deployment
- ✓ Carrier independence

Failover by M2M One

M2M One's managed failover service keeps businesses online when their primary network connection fails. Rather than relying on a single carrier, M2M One pairs a customer's existing SIMs with a secondary network. If the primary link drops, traffic automatically fails over to the secondary network, keeping connected devices and services online without manual intervention.

For businesses running critical infrastructure or customer-facing services, M2M One's service turns network resilience from a single point of failure into a managed, automatic safeguard — cutting downtime risk from everyday regional signal issues and large-scale national outages alike.

For more information, visit: www.m2mone.com.au/managed-failover/