Customer story
St John's Ambulance

Protecting people is St John's mission. Protecting St John is ours.

How a Not for Profit took control of its security to provide peace of mind for staff, volunteers and the Australian public.

Peter Bouhalis' technology career began in the 'hard science world' of CSIRO and spanned decades of innovation and leadership at the intersection of health, technology and product. When the opening appeared to lead technology and infrastructure as CIO of St John Ambulance NSW, Peter saw an opportunity help an organisation dedicated to helping others.

The aim of St John Ambulance NSW is to save lives through first aid. Whether delivered as training, advocacy, provisioning AEDs or event health services at everything from a local basketball tournament to a 3-day music festival, St John's reach is as pervasive as it is important. Their most high-profile contributions undoubtedly come from working with the community during natural disasters, including bushfires and floods, providing paramedic services and other medical support.

With so much important work to deliver in so many parts of the community, St John needed to ensure that its own safety and security were well managed.

When you're a source of trust for the public, you become a natural target for bad actors

It may be surprising to learn that an organisation such as St John is a cyber target for bad actors, but it's an increasingly common issue for not-for-profit organisations globally, especially one that collects and stores health records. The other mitigating factor for the organisation is the large number of volunteers, including the participants of their youth program. Finally, many bad actors operate under the (often correct) assumption that NFPs are underfunded or less focussed on cyber security, leading to less sophisticated levels of protection.

> "Dealing with user risks from people who aren't officially inside the organisation full time is a challenge because volunteers have their own full-time jobs. St John tries to make life easy for volunteers and uses conditional access policies to help them."
>
> **Peter Bouhalis, St John CIO**

Customer story
St John's Ambulance

> During the first month, we treat every new customer as if they're infected, to identify any gaps in their security posture. Peter was aware of the organisation's security posture and wanted to partner with Macquarie to ensure that they were completely covered.
>
> **Josh Dominguez, Macquarie Group's SOC Analyst**

"The first thing I do is my due diligence around infrastructure, security and assets, digital assets. Certainly, security was one of my first focus areas. I was looking at uplifting our security as fast as we possibly could."

For Peter Bouhalis, taking on the CIO role meant taking no excuses when it came to providing the organisation with a high level of protection, while also balancing the needs of the large volunteer workforce.

Having worked previously with Macquarie Group in similar roles earlier in his career, Peter was familiar with their industry leading customer service and partnership model. He invited them to present their credentials and approach to uplifting St John's security while modernising their defences to accommodate the unique nature of the organisation's largely volunteer workforce.

Getting on the front foot together through open dialogue

A zero-trust philosophy informed the approach taken by Josh Dominguez, Macquarie Group's SOC Analyst, during the initial assessment of St John's existing security posture and the needs of their dispersed user groups. Working from the assumption that all users, devices, and applications are untrusted and must be continuously verified before they are given access to corporate resources is a good place to start, but Macquarie's Dominguez was even more diligent.

'Bad actors' may be the ones causing damage, but security experts know the biggest threat to a company is the user base. Macquarie brought a focus on user education, along with their technical solution, to further bolster the organisation's defences.

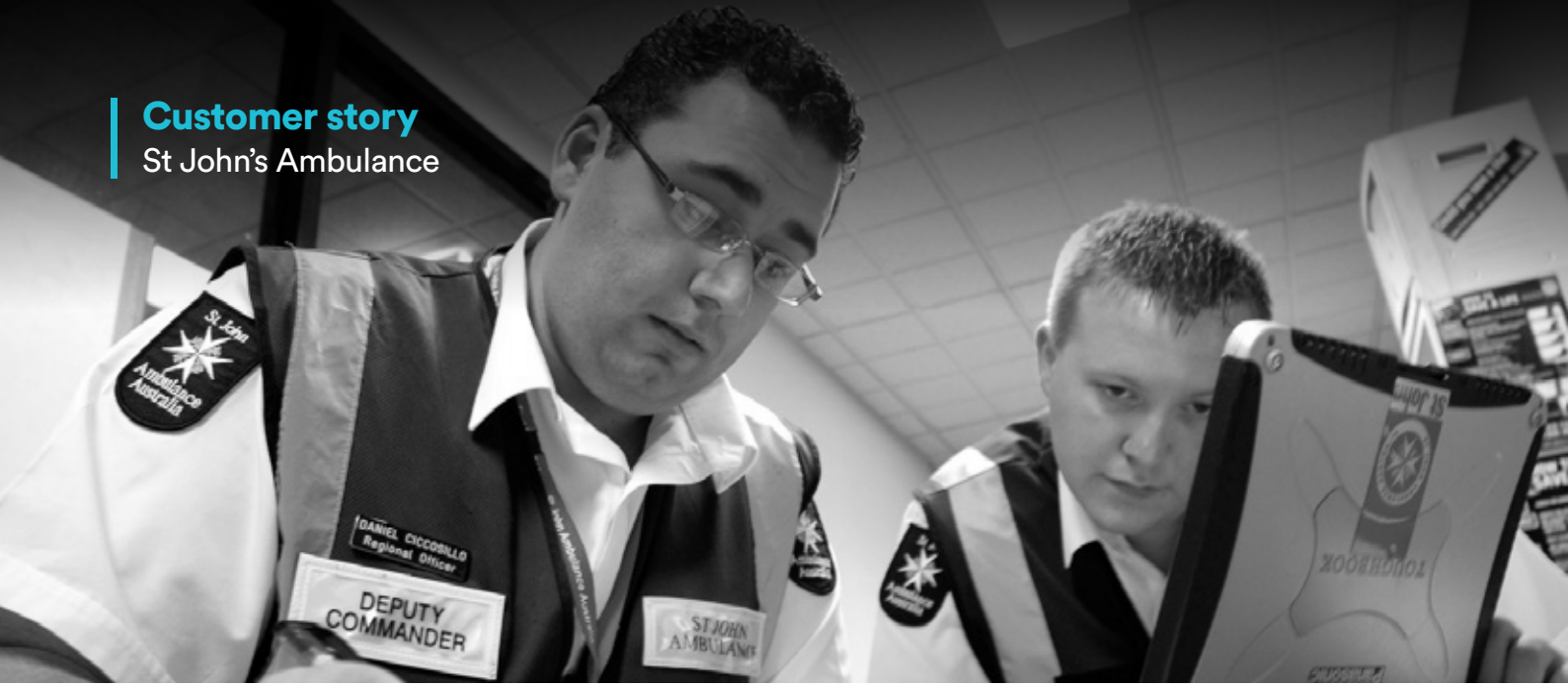
While every organisation is at a slightly different point in their security journey, moving to the cloud accelerates the need for every business leader to give security a higher priority. To help inform and educate, Macquarie provided access to their Cyber Threat Intelligence Platform, a proprietary technology resource that collates, assesses and consolidates the latest threat inputs from more than 40 data sources.

Macquarie's Managed Detection and Response solution, powered by Microsoft Sentinel, provided a dramatically improved level of visibility, using Power BI to populate dashboards with real time data. This enhanced level of transparency, monitoring and threat detection gives Peter's team at St John 'front row seats' to their own security posture.

From the CIO down, Macquarie offered partnership, collaboration and education, maintaining an 'open door policy facilitated by text, teams and voice call access that ensured the St John team always felt consulted and supported.

"Having a trusted partner like Macquarie who are so responsive and available is an absolutely vital tool for any team wanting to remain in control of their security. Particularly now that threats can emerge and evolve, quite literally, in a matter of days." says Peter Bouhalis, St John CIO.

Customer story
St John's Ambulance



The Solution

Delivering proactive Managed Detection and Response (MDR) requires the confluence of the right people, bringing a proven technology stack and process to deliver advanced monitoring capabilities.
The Macquarie Cloud Services MDR solution includes:

- Industry leading Cyber Threat Intelligence (CTI) platform, that supercharges our capabilities to identify threats in real time.
- Comprehensive detection logic, that is built over years of experience delivering security monitoring to enterprise and Government clients.
- Comprehensive operational and executive dashboards aligning security metrics to business priorities.
- Industry leading security frameworks including MITRE ATT&CK
- Microsoft Sentinel, a cloud native SIEM, bringing best practices in the domain of Cyber Security.

Need to protect your people? Find the people who want to protect you.

For an industry veteran like Peter, coming to a NFP organisation like St John represented a new operating landscape, but also a rewarding opportunity.

> It's really about giving back to the community. I was motivated to do something that's worthwhile for a company that's very, very well respected and does a lot of work in the community.
>
> **Peter Bouhalis, St John CIO**

Peter certainly lived up to his own promise, taking St John's cyber security defences to Essential 8 Level 3 – a level that has been independently audited and constantly monitored. The key was to find a security partner that had not only the experience and the skills, but also the willingness to collaborate and partner for the long term.

"It is difficult for small organisations to hire their own cyber security personnel. It can be doubly challenging for NFPs to attract and retain experienced people with both technical and interpersonal skills. Macquarie is my source for this high-level security talent and they consistently bring both new skills and proven experience to the table." Peter Bouhalis, St John CIO

For St John, contracting out security services to a trusted partner like Macquarie has proven to be the ideal solution, ensuring there is no internal conflict of interest and providing constant real-time access to specialised expertise.

If you're looking for a local security solutions provider who has the expertise to safeguard the growth of your business, you need to put Macquarie Cloud Services on your shortlist. Get in touch our experts today.

macquarie CLOUD SERVICES

1800 004 943
macquariecloudservices.com

Gold Microsoft Partner
Azure Expert MSP