Customer story
Cafs (Child and Family Services, Ballarat Inc)

For Cafs, a safe community requires cyber security.

Not all data breaches are created equal.

We all know that the impacts of a successful data breach or cyber attack on any business can be devastating. They can also be devastating for the people who are attached to any stolen or leaked data.

Of course, there are the annoying administrative tasks of changing passwords and cancelling cards. The unluckiest people may find themselves dealing with identity theft, damaged credit scores and other distressing scenarios.

No organisation wants to be responsible for their customers or employees suffering the impacts of compromised data and cyber crime. However, for some organisations the stakes are even higher. What happens when the data is attached to the most vulnerable people in the community?

For Chris Hunter, Cyber Security & Infrastructure Specialist at Cafs, it's a question that motivates him every day. As an independent community service organisation, Cafs (Child and Family Services, Ballarat) supports more than 6,500 clients across regional Victoria every year. The team delivers more than 50 services to people when they need it the most - including housing and homelessness services, family violence intervention programs and early childhood support.

"Given the nature of what Cafs does, much of the information we store is very sensitive," said Chris. "People trust us with that information, and a breach could have very serious consequences for individuals and families.

"For Cafs, it would mean a significant loss of trust and reputation in the community, and we simply can't afford that."

Security keeping pace with transformation.

Like many other organisations, Cafs accelerated its existing strategic digital transformation agenda with the onset of COVID. While the move towards a more consolidated systems architecture and infrastructure was already underway as part of a multi-year strategic plan, when 2020 arrived everything suddenly became urgent.

Thankfully, the Cafs leadership group did not need to be convinced of the need to invest in cyber security to match the acceleration towards digital tools and services.

"Being cyber resilient to protect people today is one of our key strategic items, but it's also about leveraging the opportunity of technologies such as automation and artificial intelligence (AI) down the track," said Chris. "We know these technologies can make service delivery better and easier - but you need to have the right foundations to support all the data, and they need to be secure."

To outsource, or not to outsource?

For Chris, it was never really a question of whether to build cyber security capabilities in-house.

"We have a small ICT team, so we rely on external partners to help deliver certain functions and capabilities - particularly when specialist skill sets are involved," said Chris. "This allows us to remain lean and pivot quickly as required."

"I started researching Security Operations Centre (SOC) and Security Incident and Event Management (SIEM) services, and Macquarie Cloud Services emerged as one of the leading Microsoft Security partners in Australia."

> Given the nature of what Cafs does, much of the information we store is very sensitive. People trust us with that information, and a breach could have very serious consequences for individuals and families.
>
> **Chris Hunter – Cyber Security & Infrastructure Specialist at Cafs.**

Customer story

Cafs (Child and Family Services, Ballarat Inc)

With cost and value always a consideration in the NFP sector, Cafs is moving towards consolidation of its investments in the Microsoft ecosystem, as far as possible. Thus, a partner with strong expertise in Microsoft products was required.

Technical solution overview.

1. A cutting-edge Cyber Threat Intelligence (CTI) platform, equipped with extensive real-time threat detection capabilities.
2. Robust operational and executive dashboards offering complete, real-time access to event and monitoring data.
3. Implementation of Azure Sentinel following best practices, complete with an extensive repository of analytical rules and supporting automation playbooks.
4. Round-the-clock availability of security analysts for mission critical detection and response and continuous governance and strategic support.
5. Valuable guidance and policy recommendations to enhance cost-effectiveness and overall value proposition.
6. Streamline Cafs' tooling to leverage the full potential of Microsoft's Extended Detection and Response (XDR) capabilities unlocking the inherent synergies with Azure Sentinel. Included establishing a cohesive set of security tools and governance, as well as facilitating the implementation of a Zero Trust reference architecture throughout the entire ecosystem.

"For NFPs, the Microsoft ecosystem offers a lot of value and capability for the right price," he said. "We were so impressed by Macquarie Cloud Services relationship with Microsoft."

Other key considerations for Cafs were flexibility and understanding of the NFP operating environment.

"Most importantly, the team at Macquarie Cloud Services took the time to understand our business and requirements as an NFP, which other providers didn't really bother to do.

"They were also willing to be really flexible in the commercial arrangements, helping us to make the business case with key stakeholders and get the investment over the line," said Chris.

Results.

Peace-of mind has so far been the most valuable outcome for the Cafs team as a result of the partnership with Macquarie Cloud Services, according to Chris.

"The Cyber Threat Intelligence Platform correlates over 40 feeds, which gives us access to advanced threat intelligence, the latest threat detection and response techniques," he said.

"This means we've been able to draw on the vast operational experience Macquarie Cloud Services has gained from securing other organisations. Right from the time we were onboarded, we've seen real-time alerts and captures of real events within five minutes.

"The reporting dashboards have really helped me speak the right language to the Cafs leadership team and board, particularly when it comes to articulating the benefits of reducing risk.

"Finally, from a personal perspective, I'm no longer overwhelmed by the process of sifting through and managing email alerts, because I trust the team to manage it."

"Overall, I have more peace-of-mind as the leader of the IT team - and so do the Cafs leadership team and Board," Chris concluded.

A message from Cafs to other NFPs.

Sadly, NFPs are an attractive target for bad actors. There are a few reasons for this, including the perception that many lack the funding or skills to maintain a robust security posture. Whether that perception is justified or not, we do know that many organisations right across the economy are struggling to keep up with the ever evolving cyber security landscape - let alone resourcing a robust in-house cyber security team. (According to our calculations, it takes at least 12 highly qualified staff to run a full-time Security Operations Centre.)

Chris strongly urges senior IT staff at NFP organisations to take charge of driving investment into cyber security strategy - or risk disastrous consequences.

"Cafs is a trusted advisor to vulnerable people in our community, and we have a 24/7 mission critical mandate. We simply can't risk any sort of breach or attack, so investment in security is non-negotiable.

"My best piece of advice is don't assume a comprehensive managed service is beyond the reach of your budget. If you find a partner who is focused on trust, communication and flexibility - there are always ways to make it work.

"With the support of Macquarie Cloud Services, Cafs is not only highly secure - we've also unlocked a level of agility and flexibility, as well as freeing up our focus as an IT team to do what we do best.

"That is, supporting Cafs to deliver better, more secure services to the people of regional Victoria."