# McKenzie Aged Care Group keeps finger on the pulse with Sophos MTR

Established from humble beginnings in September 2001 with an aged care facility called the "Armitage Manor" in the inner Melbourne suburb of Windsor, sisters Sally and Mary-Ann McKenzie expanded their vision to "McKenzie Aged Care Group" (MACG). With 17 residential aged care facilities and two retirement villages across Queensland, New South Wales and Victoria, MACG has grown to become one of Australia's leading privately-owned aged care and retirement providers.

## CUSTOMER-AT-A-GLANCE

McKenzie AGED CARE GROUP

**McKenzie Aged Care Group**

**Industry**
Aged Care (Health)

**Sophos customer**
Since 2018

**Website**
www.mckenzieacg.com

**Number of Users**
Approximately 2,300 staff across Queensland, New South Wales and Victoria

**Sophos Solutions**
Sophos MTR, Sophos Endpoint Protection Sophos Intercept X, Sophos XG & XGS Firewall, Sophos RED, Sophos Email Security, Sophos Phish Threat, Sophos Cloud Optix, Sophos Encryption, Sophos Mobile (device management), Sophos Switch (proof of concept)

*"Because the healthcare industry contains a large quantity of sensitive information, it is a lucrative target for any cyber criminal," says Corrigan. "Care is so dependent on technology and if there are any disruptions, it will be a huge detriment to operations and resident care. Lives are at stake. We need to have visibility on the entire playing field and that's just not possible on our own."*

Peter Corrigan, General Manager, ICT, McKenzie Aged Care Group

## Challenges

- Required a sophisticated cybersecurity solution that leveraged artificial intelligence (AI) and machine learning (ML) to help defend against advances in cyber threats.
- Needed a proactive approach to mitigate cyber risk by leveraging an outsourced professional cybersecurity response team.
- Multiple layers of security would be required to provide the levels of protection to support the business.
- Unified reporting and dashboards, simple and intuitive.

## How do you make people a priority when you're a highly targeted sector?

The healthcare industry in Australia has consistently been reported in the Notifiable Data Breaches Scheme as the sector most affected by cyberattacks. This result was no surprise to McKenzie Aged Care Group (MACG), as its own workforce is required to complete mandatory cybersecurity training as part of an annual compliance program.

To ensure staff could continue focusing on their core purpose of caring for residents, Peter Corrigan, General Manager, ICT, McKenzie Aged Care Group, had always relied on external providers to meet MACG's cybersecurity needs. As the healthcare industry grew as a goldmine for cyber attackers, Corrigan knew MACG required a cybersecurity solution that would actively protect the business without the need to constantly involve workers and distract them from their day-to-day operations.

"There is a lack of general cyber awareness across the industry," said Corrigan. "As aged care's main focus is to support individuals within the residential facilities, there is a certain stigma that the industry is not as astute with technology as other sectors may be. We put a lot of emphasis on ensuring we have the internal skills and capabilities in place to strengthen our cybersecurity acumen, which can add to the mountain of tech challenges we need to overcome to successfully defend against attacks."

*"Being protected by Sophos gives us a level of comfort. Just knowing that if any device on our network or inside a facility is infected, it will be brought to our attention, and we know it will be dealt with appropriately by the MTR team. Whether the threat is quarantined, removed, or escalated to invoke incident response plans. The business has become much more resilient with Sophos MTR. It definitely helps us sleep easy at night."*

**Peter Corrigan, General Manager, ICT, McKenzie Aged Care Group**

While it's important to defend against external attackers, aged care providers still need to ensure internal compliance to minimise the risk of human error. With increased reliance on internet-enabled services, storing and processing sensitive data, organisations may be distracted by ongoing digital demands, leaving them vulnerable to cyber attacks.

## How do you implement a cybersecurity solution yet keep things simple?

With minimal internal security capabilities, leaning on outsourced cybersecurity experts was paramount. Corrigan knew he needed one vendor that would tick all the boxes, whilst still maintaining a layered approach to protection. It was not feasible to deploy various solutions from multiple vendors that operate in silos and then manually piece together a strategy to connect the dots to make sense of everything.

"We want staff to continue to focus on the care of people, not technology. For us, the technology needed to essentially be invisible for our team to effectively do their jobs," says Corrigan. "There is no way that we could remediate cyber threats inside our environment, based on our skills, nor would we be able to react quickly enough."

In search of a comprehensive cybersecurity platform, Corrigan turned to Sophos Managed Threat Response (MTR) – a fully managed threat hunting, detection and response service. Sophos MTR provides MACG with a dedicated 24/7 security team to neutralize the most sophisticated and complex threats by monitoring their systems in real time, proactively identifying and isolating threats.

"Sophos helps us prioritise people. Before Sophos MTR, I didn't have a clear view of what was moving across our digital landscape, if our policies were enforced and who was sending what data in and out of the organisation. Now, we have the control and visibility, backed by metrics."

## What are the benefits of working with Sophos?

Having an existing relationship with Sophos made it a seamless process to expand the layers of security required for MACG. Data loss prevention was a major focus for Corrigan, considering the sensitive information held on MACG's network.

"Sophos doesn't take a cookie-cutter approach," says Corrigan. "Although the Sophos MTR team continues to help identify threats that we may be unaware of, the collaborative nature of this relationship allows us to flag industry-specific threats to create a tailored solution for us."

"For example, as part of the coronavirus pandemic, an Individual Healthcare Identifier (IHI) is found on vaccination certificates, and this is sensitive information. We spoke to the Sophos MTR team on creating a policy that would stop any information pertaining to the IHI from leaving the perimeter of our information systems. It wasn't something that initially existed, however, within a couple of weeks, Sophos was able to implement the solution. Now we have email and endpoint control policies allowing us to demonstrate compliance."



SOPHOS

2022-03-14 CCS-EN (NP)