brennan_

Brisbane Catholic Education
teaching · challenging · transforming

BCE Reduces Cybersecurity Risks with Azure Sentinel

A Microsoft Azure Case Study

About Brisbane Catholic Education

Brisbane Catholic Education (BCE) is a learning community of all involved in diocesan Catholic schools and the staff of the Brisbane Catholic Education Office. With over 140 schools, Brisbane Catholic Education provides quality teaching and learning outcomes for Prep to Year 12 students.

The Archdiocese of Brisbane covers a geographical area that includes most of south-east Queensland, and BCE employs around 10,000 people throughout the region including teachers, administrative and technical support staff, IT and HR professionals.

At a glance

Industry
Education

Company size
100+

Country
Australia

Business challenge

An increase in the number and frequency of cyber security events was overwhelming BCE's internal operations team and leaving the school network at a high risk of security compromise.

The solution

BCE deployed Azure Sentinel; a solution which integrated easily with their existing Azure environment and maximised their existing Microsoft investments.

The Results

The successful integration of Sentinel has enhanced BCE's security capabilities, reduced the time and cost involved in responding to threats, and ultimately reduced the risk of a successful cyber-attack.

The Situation

As part of overarching security controls deployed within their IT environment, Brisbane Catholic Education conducts regular cybersecurity reviews to highlight risks and gaps in security capabilities. These reviews are designed to ensure that BCE's existing investment in Microsoft infrastructure is being used as effectively as possible to mitigate these risks. The reviews often result in new features being enabled, to enhance BCE's existing Microsoft 365 and Azure investments.

The Challenge

During one of these reviews, it was noted that an increase in the frequency and volume of events related to attacks on accounts and identities was overwhelming the BCE internal operations team and leaving them at a high risk of security compromise.

To bolster their security posture and address the situation proactively, BCE identified the need for a dedicated Security Operations Centre (SOC) to investigate, respond to, and mitigate events within their environment.

With a desire to make the most of their existing investments in Microsoft and Azure, as well adjacent security controls and services, BCE wanted a solution that could monitor and respond to security alerts on a 24/7 basis across their environment.

The Solution

During a discovery process undertaken by the Cybersecurity Team at MOQdigital (a Brennan company), during which BCE's cybersecurity needs were thoroughly reviewed, the team recommended deploying Azure Sentinel as part of their Sentinel Managed Service.

The solution would integrate with BCE's Azure Environment and include the collection of log sources from outside the Microsoft and Azure environments, providing additional value and insight.

With built in AI and Machine Learning capabilities, and leveraging Microsoft's significant investment in security, this solution would be managed, developed, and enhanced by a dedicated 24/7 SOC team, and include the following:

- Security Incident Response – Responding to threats based on priority, investigating incidents using Sentinel's advanced log correlation and visualisation tools, and producing post-incident reports for high profile security incidents.
- Threat Hunting – Actively seeking new or unknown suspicious activities, as well as patterns similar to recent events, leveraging Sentinel's powerful entity explorer and guided hunting notebooks.
- Enhance – Provide a continual cadence on the review and posture of the security capabilities of BCE, ensuring that adequate protections and controls are put in place to stay ahead of evolving threats.
- Security and Cost Management Report – Regular security incident reports, including a forecast on their Azure investment and recommendations.

The Result

Brisbane Catholic Education was able to successfully integrate Azure Sentinel into their environment, and together with the SOC team, provide 24/7 mitigation of the risks associated with identity compromises and other potential cyberattacks on the BCE environment.

"Our cybersecurity capabilities have been greatly enhanced" says Jeff Peters, BCE's Manager, Information Systems. "We are now able to respond quickly to security alerts and keep our environment secure."

Following the adoption of Azure Sentinel, not only has BCE reduced the time and cost involved in responding to threats, but also increased the accuracy of event information and reporting - ultimately reducing the risk of a successful attack on the BCE's data, applications and most importantly, its users.

Strengthened security posture

Reduced the time & costs involved in responding to threats

Increased accuracy around security event information & reporting

brennan_

The Brennan Experience

Brennan is uniquely positioned to transform, deliver, and manage your complete IT environment - so your people can have a truly seamless IT experience, wherever they are working.

We provide powerful technology solutions for Australian organisations, with a portfolio of services that ranges from strategy and advisory, to application development, to end-user support, and more.

Our teams are crazy about delivering an exceptional customer experience for our clients, which is why we continue to invest in our people, systems, and automation. This has resulted in us achieving a world-class Net Promoter Score of +80.

Get in touch with us today to see how we can help your organisation.

Speak to us today

brennanit.com.au
1300 500 000
sayhello@brennanit.com.au

Find us here