



University of Southern Queensland Teaches Cybercriminals a Lesson With Sophos MTR

Founded in 1967, University of Southern Queensland (USQ) has over 50 years of experience in educating students from around the globe. A recognised leader in online and blended education, USQ is renowned for its supportive environment and student-focused commitment to learning and teaching.

CUSTOMER-AT-A-GLANCE



University of Southern Queensland

Industry
Education

Customer
Since 2010

Website
<https://usq.edu.au/>

Number of Users

2500 employees in Australia
27,500+ students from around the world

Sophos Solutions

Sophos Managed Threat Response (MTR) for Endpoint and Server
Sophos Phish Threat
Sophos Device Encryption

'We ran a proof of value exercise with a number of vendors, but Sophos was the clear winner in terms of the benefits and peace of mind it would bring to our team.'

Scott Sorley, Executive Director of ICT Services

Business Challenge

Needed to ensure proactive protection, particularly throughout COVID-19 when many staff were working remotely.

Required a cybersecurity solution that could face the evolving threat landscape especially targeting the education sector.

When should cybersecurity be more than just detection?

As an organisation that operates in a sector that has seen several high-profile cyberattacks in recent years, University of Southern Queensland (USQ) doesn't underestimate the importance of cybersecurity and the need to be proactive. As an early adopter of online learning (which meant the university didn't miss a day of learning during COVID-19 restrictions) its cybersecurity posture has, for a long time, been very strong. However, for Scott Sorley, Executive Director of ICT Services and Luke Drury, Cybersecurity Manager at USQ, it is important to remain proactive to defend against the modern threat landscape.

"The threat landscape moves at a rapid pace, so it's important we're on the front foot and not waiting for something to happen," said Drury.

After identifying what was needed, Sorley and Drury conducted a rigorous evaluation process, speaking with a number of vendors. They ultimately decided Sophos' [Managed Threat Response \(MTR\)](#) – a fully managed threat hunting, detection and response service that provides organisations with a dedicated 24/7 security team to neutralise the most sophisticated and complex threats – was the perfect service for the university's requirements.

"What we were looking for wasn't just about the detection of threats, but also the response capability."



'We wanted to invest in a service that ensured we were being proactive in our cybersecurity approach; a service that was going to not only detect, but respond to these threats, before they became a problem for us.'

Luke Drury, Cybersecurity Manager, University of Southern Queensland

How do you stop a pen tester in their tracks?

While confident Sophos MTR was the right choice, Sorley and Drury did not expect the service to work as well as it did. Initially, MTR was given restricted access where USQ's IT team would review all threats flagged. After seeing how accurate and effective the service was (there were no false positives), MTR team members were given access to manage and isolate threats themselves.

"It's important we make smart investments that deliver real value to the organisation, but we didn't anticipate the value to be as good as what it has been," conveyed Drury. "We never expected to be able to take a step back and give MTR full autonomy, without ongoing intervention from our end—but that's the way it is."

Drury recounts a time he put MTR to the test by hiring third-party penetration testers, without notifying the MTR team. To his—and the penetration testers'—great surprise, MTR passed with flying colours.

"MTR picked the pen testers' pockets. The penetration testers had no answer or recourse for being stopped. Every time the testers tried anything, MTR isolated the endpoints and notified us immediately of what was happening. The Sophos MTR called and spoke to us in front of the penetration testers, who were still shocked they couldn't find a way in. That was the very point we knew we could absolutely trust the Sophos service."

What are the benefits of working with Sophos?

By partnering with a proactive service, USQ has full assurance it is protected by a team of highly trained technical support representatives that "has its back". MTR is also cost efficient. It not only eliminates the cost of hiring several full-time employees, but it also frees up existing resources from performing such things as admin, analysis and reporting to focus on other priorities.

As the Sophos MTR team understands USQ's environment, it can collaborate directly with the university rather than operate in a transactional manner, making it a true partner to the organisation.

"Sophos MTR allows our resources to do more. We trust the MTR service is doing its job and that the Sophos team will be in touch if something needs to be discussed. When we see the MTR team calling or emailing, we stop and give them our full attention, because we know it's important. The level of partnership we have with Sophos is unprecedented," concluded Drury.

'Sophos MTR allows our resources to do more. We trust the MTR service is doing its job and that the Sophos team will be in touch if something needs to be discussed.'

Luke Drury, University of Southern Queensland

To find out more about Sophos solutions, visit www.sophos.com or email sales@sophos.com