

Regional Healthcare Provider in Australia Sees Nearly 70% Reduction in Mean Time to Respond

August 2026, Dave Gruber, Principal Analyst

Case study

Business impact results

- **60% reduction** in the amount of time spent investigating false positives
- **Nearly 70%** improvement in mean time to respond
- **18% risk reduction** in a five-month period
- **Simplified** Payment Card Industry Data Security Standard (PCI DSS) compliance preparation
- **Simplified** reporting for board of directors

Technology provider: **TrendAI™**

Customer: **Mater Group, 10,000-plus employees**

Industry: **Healthcare**

Country: **Queensland, Australia**

Introduction

Mater Group is a major healthcare provider in Queensland, Australia, originally founded by the Sisters of Mercy in 1906. It operates under four key entities: Mater Health, Mater Research, Mater Education, and Mater Foundation.

Mater Health has approximately 8,000 employees and serves more than 500,000 patients annually. The not-for-profit group manages both private and public hospitals.

Supporting this diverse, highly distributed environment are information systems and technologies used for every aspect of care delivery and administration. With this dependency, cybersecurity plays a critical role in ensuring the group's success as a healthcare delivery provider.

It was vital for Mater Group to architect and operate a secure 24/7 solution. It needed to build and mature its security program over time to meet the needs of a diverse, highly distributed operating environment. This led Mater Group to select TrendAI Vision One™ to secure its rapidly growing hospital system's critical data, systems, and infrastructure.



Nearly
70%
reduction in mean
time to respond

“The last thing I want our providers to worry about is IT. **I want them focused on delivering patient care.**”



Scott Hawkins,
Director of Cyber Security, Mater Group

A security lapse can compromise patient care

The complexity of healthcare creates opportunities for successful cyberattacks. Aging service delivery systems and highly distributed operational environments challenge security teams to identify assets, vulnerabilities, and risks and to mitigate the latter without disrupting care. Regulatory requirements add further challenges, as systems often operate with protected healthcare information data, with strict limitations on access control.

While the fundamentals of cybersecurity frameworks apply in healthcare, cybersecurity program development and management are particularly challenging for healthcare delivery providers. Despite a well-thought-out incident command center and thorough downtime procedures, the impact of a major incident could disrupt care at multiple levels.

Before TrendAI Vision One™

Mater Group knew cybersecurity was a priority, but it needed a strategy. It had very limited tooling and visibility across its operations and little to no cloud presence or activity apart from third-party web applications.

When Scott Hawkins came on board in 2011 as Mater Group’s Director of Cyber Security, the first thing he focused on was developing a strategy aligned with National Institute of Standards and Technology (NIST) principles and the Australian Signals Directorate (ASD) Essential Eight framework. He took a close look at Mater Group’s operating environment from a cybersecurity and digital infrastructure perspective, with the goal of elevating overall digital capabilities to enable the organization to operate as a digital hospital.

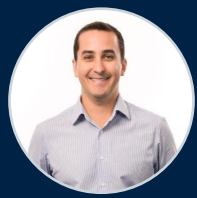
Prior to implementing this cybersecurity platform, Mater Group experienced many challenges that touched multiple business areas, such as the technical environment, resourcing, and culture. These included:

- **Limited visibility.** As a health system, Mater Group faces a core challenge: ensuring full visibility across thousands of endpoints and users that need to be secured and protected. Monitoring multiple platforms to gather consistent data on alerts, logs, and anomalies was a key issue. This fragmented approach was difficult and time-consuming to correlate security signals from different systems to get a comprehensive view of the security landscape.

- **Inefficient threat detection.** This labor-intensive approach also made it challenging to detect and respond to malicious activities promptly, delaying response times and increasing the risk of potential successful incidents. The initial primary objective was to improve visibility and response times.
- **Operational complexity.** Managing multiple systems for identifying and addressing issues requires significant manual effort. Security personnel had to switch between different point products to manually piece together information, delaying investigations. The high frequency of false positives further exacerbated the problem, consuming valuable time and diverting attention from genuine threats.
- **Talent and skill shortages.** Without a centralized system, it was difficult to allocate and train security resources effectively. Multiple teams had to be notified of each alert, leading to frequent personnel overlap and inefficiencies.

Mater sought a solution that was easier to manage, linked user identities with web activities, and provided better visibility and proactive cyber risk reduction.

“For us, having the **right partner was key** to our journey.”



Scott Hawkins,
Director of Cyber Security, Mater Group

Seeking a scalable solution to accelerate security program growth

Mater Group sought a solution that was easier to manage, linked user identities with web activities, and provided better visibility and proactive cyber-risk reduction. Early objectives included:

- Improving risk visibility into security posture and threats, enabling clear reporting to leadership.
- Driving security operations through risk-based decisions and prioritizing focus on the most critical threats.
- Boosting compliance readiness and tracking progress with measurable metrics
- Expanding visibility into operating assets and infrastructure.
- Improving mean time to respond (MTTR).

Using the NIST framework as a tool for self-assessment of maturity and progress toward objectives, Mater Group sought to map initiatives and align spending with those objectives.

From an operational perspective, the organization needed a better understanding of risks and the ability to prioritize work accordingly. Alignment with the broader line-of-business teams and executive leadership was a key objective but would require exploration. An executive communications plan was also required to ensure leadership had the visibility needed to support the security program.

TrendAI Vision One™ in action

As a healthcare provider, outages involving supporting infrastructure and endpoints are common, so Mater Group needed to address those risks. It determined that virtual patching from TrendAI™ was its best approach to begin the journey.

With a successful virtual patching solution in place, the group explored solutions to support the security operations function. Because of early successes and the strength of the relationship with TrendAI™, Mater Group adopted the TrendAI Vision One™ Security Operations (SecOps) solution with integrated XDR. It also made use of the TrendAI Vision One™ Services – Managed Detection and Response (MDR) to augment monitoring, alert investigation, and get recommendations on response actions to mitigate threats. When it comes to the actual response actions, Mater Group still maintains operational responsibility to respond to incidents, helping ensure it can evaluate and limit any potential impact to its healthcare operation.

“With TrendAI Vision One™, we have all the information we need in one console. We’ve reduced our mean time to understand (MTTU) the threats in our environment. Before, we were flying blind. Now, we identify, investigate, and resolve alerts in real time in the dashboard.”



Scott Hawkins, Director of Cyber Security, Mater Group

Mater Group is using TrendAI™ as a single provider wherever possible, with telemetry from other tools flowing into TrendAI Vision One™ as needed. This provides visibility into complex threats across the entire environment. “Mater’s goal isn’t to work with a single provider; it is about reducing complexity and strengthening our capabilities,” Hawkins explains.

Hawkins credits TrendAI Vision One™ with providing multiple improvements to both the efficacy and efficiency of Mater Group’s security function, including:

Business impact

Mater Group reports significant improvements fueled by TrendAI Vision One™ across its entire security program, including:

- **Faster prioritization.** TrendAI Vision One™ automates Mater Group's threat research and prioritization, eliminating manual effort. Information that once took hours to locate can now be gathered in minutes.
- **Faster response.** "TrendAI Vision One is helping our team react and respond faster, improving response times by 70–80%. We've improved our ability to go from detection to proactive action," says Hawkins. "In many cases we can detect and mitigate in a single step. This makes the process both faster and more efficient."
- **Improved mean time to patch.** Over a nine-month period, Mater Group decreased mean time to patch by 72%.
- **Reduced complexity.** Consolidating the number of security tools in use with TrendAI Vision One™ has reduced management and operational complexity for Mater's security team, freeing them to focus on more strategic activities.
- **Unmanaged device discovery.** Multiple systems and resources were previously required for Mater Group to see app usage on unmanaged devices. With TrendAI Vision One™, the process is much faster and handled by a single team member.
- **Simplified compliance preparation.** Mater Group feels better equipped to meet compliance objectives using TrendAI Vision One™. The enterprise cybersecurity platform has simplified PCI DSS preparation and incident management, enabling a single team to handle it all.
- **Team efficiencies.** Mater Group estimates that matching TrendAI™'s 24/7 MDR capability would require an additional four to five full-time employees. MDR frees up the local team to more rapidly respond to alerts, in addition to enabling them to focus more on other key security activities. These include vulnerability management, threat hunting, and working with operational teams to address vulnerabilities.
- **Organizational alignment.** TrendAI Vision One™ guides the security team and extended, non-cyber operational teams to work on the right things at the right time.
- **Executive support.** While still a work in progress, hard metrics on the organization's security posture and areas of risk can now be provided to Mater Group leadership.
- **Increased organizational confidence.** Since improving the cybersecurity program, Mater Group's security team has been actively engaging with line-of-business organizations as they look at new applications, products, and digital investments. In the past, they would attempt to onboard a product, then engage the security team after the fact. Hawkins sees this as a measure of success.



“We’re seen as an enabler, rather than that necessary ‘tick box’ at the end of the process. Now, we are involved much, much earlier in the process,” said Hawkins, who believes that Mater Group is only just scratching the surface of what can be accomplished with TrendAI Vision One™.

“We have a diverse organization across the state of Queensland. In addition to our corporate areas, we have foundations and research projects, all with very different user profiles,” says Hawkins. “Many of our healthcare workers aren’t in front of a PC all day but are connecting from personal devices and whatnot. I’m excited about new functionality coming soon that will allow us to look at our assets and users within their individual organizational units, departments, and divisions. This will be invaluable for us.”

Rather than looking at new shiny tools or increasing spending, Hawkins is looking to maximize the value from the investments already made with TrendAI™. “There’s some really exciting stuff coming,” said Hawkins. “With so much on the roadmap, it can be tough to keep up with all the new features. In addition to having new visibility across our business units and divisions, we are also excited about the use of the AI companion and how that will advance the skills that my team needs.”

Conclusion

While the fundamentals of cybersecurity frameworks apply within healthcare, the level of diversity, third-party systems and solutions, strictly protected data requirements, and 24/7 critical operating environments pose significant challenges for healthcare delivery providers. These include cybersecurity program development, operations, and management.

Security leaders supporting this environment need all the help they can get to see, protect, and mitigate risk across this diverse attack surface. Trusted partnerships with cybersecurity solution providers, such as TrendAI™, support the growth and sustainability of security programs. In turn, this strengthens security posture, simplifies security operations, and eases program management as organizations grow.

The trusted relationship between Mater Group and TrendAI™ continues to grow as well, accelerating the former’s security program growth and maturity and enabling the Queensland-based regional healthcare provider to deliver quality patient care within a secure operating environment.



[Learn More](#)



©2026 TechTarget, Inc. d/b/a Informa TechTarget. All rights reserved. The Informa TechTarget name and logo are subject to license. All other logos are trademarks of their respective owners. Informa TechTarget reserves the right to make changes in specifications and other information contained in this document without prior notice.

Information contained in this publication has been obtained by sources Informa TechTarget considers to be reliable but is not warranted by Informa TechTarget. This publication may contain opinions of Informa TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent Informa TechTarget’s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, Informa TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of Informa TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.



Omdia provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

© 2026 TechTarget, Inc. All Rights Reserved. Unauthorized reproduction prohibited.