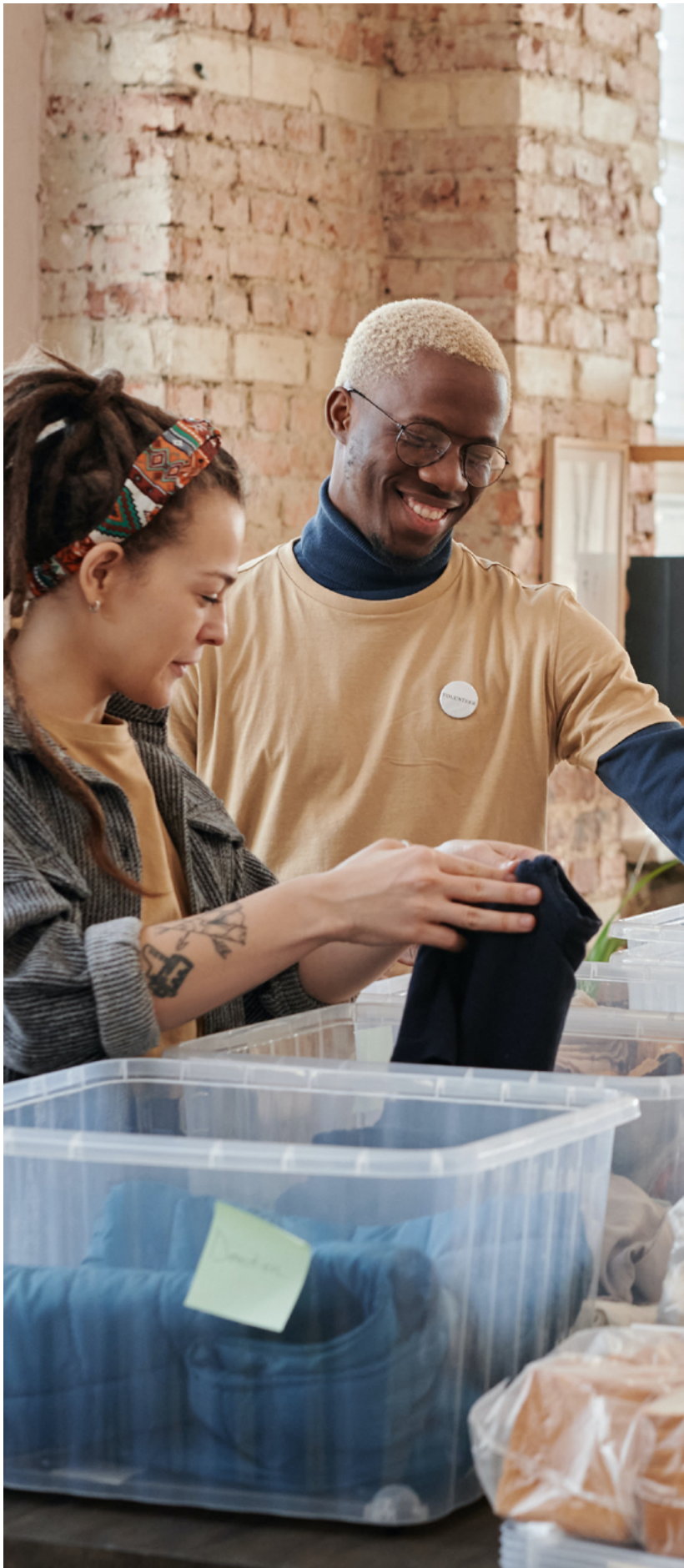
CUSTOMER STORY

RAPID7

Wesley Mission

Adds InsightVM Tools and MDR Service to Secure Its Remote Workforce



Products

- InsightVM
- Managed Detection & Response

Size

- Enterprise (Mid-Size)

Overview

The Company

Wesley Mission Queensland (WMQ) is a not-for-profit community service provider that offers community support, mental health services, aged, disability and palliative care, and retirement living across Queensland, Australia. WMQ operates as a mission activity of the Albert Street Uniting Church to provide accessible and flexible services to older people, those living with a disability or mental illness, and vulnerable children and families.

Taraiz Khan is the manager of information security at Wesley Mission Queensland, reporting to the organization's Director of Organizational Transformation. "My role is to look after everything related to cyber security; writing policies, risk management, security awareness and security operations. Our operations and IT teams also help us implement the security controls.

Our environment consists of SaaS applications, such as Office 365 and medical applications. We also have applications hosted in our data centers, which users access through a VPN," explains Khan. Khan takes a realistic approach to managing the large environment. "Our strategy is to provide a secure environment to support our staff so that they can focus on serving our clients. As a security team, we work in the background to monitor and respond if there is an incident. WMQ does an incredible job supporting Queenslanders and our team plays an integral role in supporting our frontline workers, so they can focus on what they do best."

The Challenge

Like most workforces, since the COVID-19 pandemic, the greatest security challenge WMQ faces is the shift to remote work. "We noticed an increase in cyber threats around the time people started working from home," states Khan. "The biggest issue was monitoring vulnerabilities in staff computers. We had limited visibility into what they were doing so the challenge was to respond to the incident. We particularly noticed an increase in phishing scams."

Their other major challenge is resources. "We're a relatively small team and we do not have the resources to build an in-house security operation center or have a big SOC team. From the outset our goal has always been to execute 24/7 monitoring of our environment, so if there were an incident, there are eyes on it immediately and the fastest possible resolution."

The Solution

InsightVM and MDR Are a Powerful Combination

Khan had a clear picture of the security approach he needed to address the challenges of vulnerabilities in his environment. "We knew we needed constant monitoring and after contacting a lot of vendors, we liked the Rapid7 InsightVM vulnerability management tool, in particular its live dashboard updates and the expertise of Rapid7's Managed Detection and Response (MDR) service."

Today, Wesley Mission Queensland has both InsightVM and the Rapid7 MDR service. "Vulnerability management is one of the security compliance requirements of ISO 27001," states Khan. "We also want our endpoints protected. From previous experience I knew we did not want to have too many agents. And with Rapid7, we only need one agent for both InsightVM and MDR."

The working combination of InsightVM and MDR has given Khan and team a whole new level of visibility across their widespread infrastructure. "When we first started with MDR and IVM, we could see people were trying to log in from outside Australia. We're an Australian-based organization - we don't often have people working overseas. We didn't have that kind of visibility before. That's where we see huge value in Rapid7. The rich research on threats and vulnerabilities from Rapid7 provides us with updates when there is new data or a change in our environment."

"If there are suspicious activities on the endpoint, IVM can feed all that information into MDR. We have visibility into how many vulnerabilities there are. With the live dashboard we have past data that shows the progress as well as live data so we don't have to run reports or wait for the scan to finish."

Patching is handled by Wesley Mission Queensland's IT team. "We run a meeting and give them access to IVM. They can see all the vulnerability information and can plan how they're going to patch."

> **"Before Rapid7, we knew there were cyber-attacks happening. But after we signed on with Rapid7 to help address vulnerabilities and detection and response, we see that incidents have gone down almost to zero. Small things, sure. But we have not had a single, major incident happen within our environment since we added Rapid7 to our team.**
>
> Taraiz Khan, Manager of Information Security

Adding 24/7 Experience to Their Team

Khan chose Rapid7 MDR for its SOC expertise. Before MDR, the WMQ security team did not have a clear picture of their environment. But that's all changed. Now the MDR team gives them full visibility into their whole landscape. "We can ingest a lot of logs from our firewalls, endpoint protections and our DNS Windows. We can search endpoints. We can see all of the activities happening. That was the concern, because we have a large staff working remotely. Having visibility into our entire environment is key."

One of the first things they noticed after launching the MDR service was the immediate uptick in reporting and communication from the Rapid7 team. The MDR SOC is finding and managing the most critical alerts for their small team. "The MDR team is doing threat hunting for us regularly. And if they find an issue, they inform us and escalate it straight away."

The Wesley Mission Queensland security team has gained a level of incident detection and response they had not seen before. "Since we began working with Rapid7 two years ago, we have not seen a major incident within our environment," Khan says. "The system was put to the test with a minor incident that occurred in the middle of the night where a user downloaded some malware. Our Rapid7 MDR team picked it up right away and called us at 2:00 a.m." After that incident, Khan quickly took advantage of the MDR team's expertise and 24/7 coverage and worked with them to establish an automated response procedure.

The MDR team provides critical expertise investigating incidents. "We are really pleased to have the MDR team provide insights and expertise, working side by side with our in-house security team," states Khan. Khan also points to the quality of incident reporting he receives. "Reporting is an important part of our security process and we are pleased with the quality and detail provided by the MDR team as well as remediation suggestions to stop the same thing from happening in the future."

In fact, Khan considers the Rapid7 MDR SOC a critical extension of his team. "The MDR team is always available, 24/7 to help us. We always have someone to talk to whenever we need to. We can send an email. We can call the number. This is what we like about Rapid7."

24/7

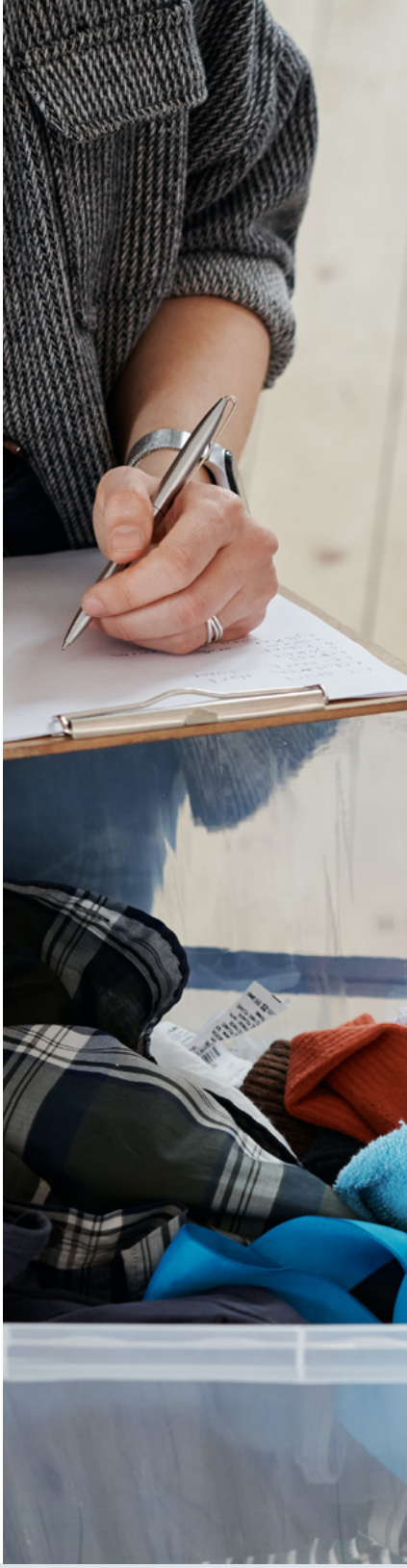
MDR Team Coverage

RAPID7

A New Level of Security

Khan now looks out over his environment and sees a whole new level of security. "We've built a team and brought in a new level of controls. Before Rapid7, we knew there were cyber-attacks happening. But after we signed on with Rapid7 to help address vulnerabilities and detection and response, we see that incidents have gone down almost to zero. Small things, sure. But we have not had a single, major incident happen within our environment since we added Rapid7 to our team."

"Rapid7 is really helping us reduce a lot of risk in terms of cyber and IT. We have visibility," concludes Khan. " That's very important for us. And, I know if anything happens, the MDR team is there to help us."



About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attackers methods. Trusted by more than 10,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CUSTOMER SUPPORT

Call +1.866.380.8113

To learn more or start a free trial, visit: https://www.rapid7.com/try/insight/