RAPID7

CASE STUDY

Rapid7 Managed Services Help Australian Lender Minimize Risk and Maximize In-House Resources

About Resimac Group	Challenge	Solution
Industry: Finance	Suffered a security incident that went undetected by staff.	Rapid7 Managed Services covers over 80% of Resimac Group's requirements.
Size: 200 Employees	Lacked staff necessary to mitigate potential threats throughout a 24-hour span.	Around-the-clock monitoring allows employees to streamline high-priority alets.
Products: Managed Services		

With a history that dates back to 1985, Resimac Group is one of Australia's premier non-bank lenders. Serving 50,000 customers across Australia and New Zealand, the firm has over three decades of experience delivering home finance solutions. Head of IT Operations, Rob Mihalek, and Cybersecurity and Engineering Lead, Brad Smith, work with a small in-house team of three service desk staff and two engineers, plus a handful of contractors.

Alongside Rapid7, the firm runs a variety of security tools including next-gen AV, web application firewalls, next-gen firewalls, and email security gateways from industry-leading vendors.

The Challenge

Financial institutions around the world have always been an attractive target for hackers keen to get their hands on sensitive customer data, launch online extortion attacks, and interfere in internal business processes to siphon away funds. Even in the United Kingdom, one of the most mature global financial services markets, breaches reported to the regulator soared by 480% in 2018 according to RPC.

As part of its customer offerings, Resimac issues a credit card, which means that it is also bound by strict PCI compliance rules. This puts extra pressure on an in-house security team already tasked with keeping escalating threats at bay. With just a handful of staff, Mihalek and his team manage a footprint of approximately 600 assets for the 300+ employees across Australia, New Zealand, and Manila.

Needing extra help to support its PCI compliance program—and drive best practices to improve security across the organization—Mihalek sought the help of an outside managed security services provider back in 2017. The decision was underlined by a security incident the firm suffered, an incident Smith claims would have been picked up by a managed security service if one had been in place. But there were also good financial reasons for outsourcing security, says Mihalek.

"If we have just one full-time cybersecurity employee, it's impossible to stretch that one person across a 24-hour span. And for us to build a SOC internally for the size of our business just wouldn't be economically feasible," he says. "So outsourcing was a key necessity."

Why Rapid7?

Using the CIS Top 20 as a benchmarking tool, Mihalek hired a third-party security firm to perform assessments of several providers. They found Rapid7 covered over 80% of their requirements via Rapid7's portfolio of managed service offerings: Managed Detection and Response (MDR), Managed Vulnerability Management, and Managed AppSec.

MDR is Rapid7's flagship service for around-the-clock threat monitoring, incident management, and response, leveraging Rapid7's expert threat hunters, SOC analysts, and the InsightIDR cloud SIEM platform. Managed AppSec enables teams to leverage the power of InsightAppSec, Rapid7's leading DAST solution, and Rapid7 experts to perform scan management, vulnerability validation, and application pen testing. And Managed Vulnerability Management enables customers to leverage their InsightVM or Nexpose investments while saving operational resources. Underpinning each offering is a dedicated security expert, the Customer Advisor (CA), who provides guidance to the Resimac team and ensures the security program continues to mature.

Taking the Strain

All three managed services run like clockwork, keeping Resimac's IT systems and data more secure and more compliant at all times. Mihalek and his team check in on their AppSec program and InsightVM around once per month for basic housekeeping, while they consult InsightIDR every day to check the latest breaking alerts.

Outsourcing the management of InsightAppSec and InsightVM has significantly reduced the workload for Resimac's stretched in-house IT team, while also streamlining internal processes.

"The main benefit with Managed Vulnerability Management is removing the management overhead for us; it's a big time-saver. We cover the top 25 vulnerabilities report by asset and vulnerability, and then use the remediation plan that InsightVM spits out. We then go through and make the necessary updates and changes," explains Smith.

"It's simplified things for us. Before we were just using a vulnerability scanner, which only tells you what the vulnerability is and how to fix it. But with InsightVM and our Customer Advisor's guidance, we get a remediation plan and key focus areas. Risk scoring is another good component that assists us in targeting the vulnerabilities we need to."

Resimac is using the Managed AppSec service to run scans across five core web applications. According to Smith, the service saves time and resources by whittling down findings from the 600 or 700 vulnerabilities reported it may find per site following a scan to just 20 or 30 validated vulnerabilities that the team need to action on. All that's left is to work alongside the development team on what to prioritize in their SDLC for the upcoming release.

"Sleeping easier at night is one aspect, but it's about being more proactive about things. It's knowing what the landscape is, being able to report on what we don't know, and to sort, categorise, and prioritise particular styles of threats. It has been an eye-opener for us, particularly because we don't have a CISO in the business."

Extending Maturity Company-Wide

When it comes to the level of engagement with all three managed services, Mihalek and Smith praise the CAs, their single point of contact in the Rapid7 SOC, who can be contacted quickly and easily to solve any issues or escalations. But beyond this, the real strength of the service has been in helping to improve Resimac's overall security maturity.

"We catch up with one of our CAs regularly, and the conversations we have aren't just purely around the MDR service—they might be about new vulnerabilities and other things in the industry that have popped up. So we can leverage their knowledge and experience to get more security information," says Smith.

"Because the CAs sit across numerous other customers, we can also see what other people in the industry are doing, what's working for them, and adopt some of those practices."

In this way, Resimac's CA was able to suggest and quickly roll-out some custom alerts for a new File Integrity Monitoring (FIM) feature in MDR, which were originally developed for another Rapid7 customer, a large law firm.

The results speak for themselves. An initial assessment of the firm's security posture two years ago revealed a maturity rating of 1.5/5. Today it has risen to between 2.5 and 3. Even more impressive, Resimac has been able to accelerate its efforts to deliver this uplift in maturity a year ahead of schedule.

"Sleeping easier at night is one aspect, but it's about being more proactive about things. It's knowing what the landscape is, being able to report on what we don't know, and to sort, categorise, and prioritise particular styles of threats. It has been an eye-opener for us, particularly because we don't have a CISO in the business," concludes Mihalek.

"Because of Rapid7 we can focus on the goals of the business rather than having to manage and plough through notifications, alerts, and problems found by security tools. Thanks to Rapid7, one thing we've not experienced is security fatigue."

To learn more about Rapid7's Managed Services, visit www.rapid7.com/services/managed-services/.