



CASE STUDY: RMIT University

RMIT partners with IPsec to protect the security of one of Australia's most revered places of learning



| | |
|-----------------|--|
| Employees | 5,000 |
| Students | 82,000 |
| Founded | 1887 |
| Headquarters | Melbourne VIC |
| Locations | 5 |
| Market Vertical | Tertiary Education |
| URL | www.rmit.edu.au |

Executive Summary

Securing digital assets places great pressure on the stretched resources of every IT department. The size and complexity of the operating environment is directly proportional to the number of potential risks that IT professionals must confront. RMIT security staff were swamped with an increasing workload to maintain their security posture and this was adversely affecting service delivery and detrimentally affecting their reputation within RMIT. By collaborating with IPsec, the University alleviated some critical workflow bottlenecks and solved operational goals. To meet RMIT's strategic objective of monitoring security safeguards 24*7*365, IPsec implemented their industry leading managed service. Providing this level of protection using internal resources would have meant increasing headcount, requiring a sizeable increase in payroll budgets. IPsec helped RMIT achieve enhanced levels of overall security at a fraction of the cost of resourcing this service internally.

- Reducing the security workload has enabled a greater focus on providing consistent and predictable service delivery to RMIT stakeholders
- Providing around-the-clock security monitoring was prohibitively expensive compared with partnering with the IPsec security team
- Complex environments are challenging for security personnel to secure and protect
- RMIT's Information Services group has garnered prestige by resolving security bottlenecks that affected service delivery throughout the entire supply chain
- The partnership has injected high-level security skills into the organisation with IPsec employees now treated as valued and trusted members of the RMIT security team

"IPsec's continuous security monitoring and technical expertise has contributed to improving RMIT's security posture"

Ben O'Neill - Deputy Director ICT Infrastructure Delivery
RMIT University

Business Driver

Like all educational facilities, RMIT University's budgets were under continuous cost pressures with users demanding better service levels combined with uninterrupted service delivery. The University's security staff were overloaded with the sheer volume of work, particularly the firewall team who were swamped with additions, moves and changes to ensure the comprehensive protection of their security perimeter. Another challenge was the IT leadership team's desire to provide 24*7*365 security monitoring. If a volatile security scenario arose outside of standard business hours then escalation and remediation procedures may not have met the IT department's high quality and service standards. After an exhaustive assessment of security service providers, IPsec were asked to review the environment and develop an actionable remediation plan to help solve RMIT's concerns.

IPsec Business Solution

IPsec's first task was to discover RMIT's security environment and learn how processes and technology interacted. When this extremely complex task was completed the onerous job of auditing firewall rules began. Managing firewall and IPS rules is demanding work, made even more challenging because of the sheer size and reach of the University's network. Harmonising the firewall and IPS rule-sets was critical to keep the rule base clear and consistent. IPS parameters were finely tuned to reduce false positive alerts. Having established a security baseline with the gateway infrastructure, phase two of the project commenced. In spite of the diligent efforts of RMIT's IT Executives, failings in service levels were still present. Implementing IPsec's 24*7*365 security monitoring service, filtered and flagged important security alerts and provided a 15-minute response time for high severity issues. This reduced the staff workload and helped improve user satisfaction levels.

Summary

Incremental improvements in RMIT's security posture have been achieved since their relationship with IPsec commenced. Firewall and IPS throughput depends on efficient rule-sets and by simply cleansing and streamlining these, noticeable network performance improvements have been delivered. Even a minor system change or hardware tweak can improve the security so vital in protecting the privacy of RMIT stakeholders. RMIT understood the business benefits of the managed services provided by IPsec but quickly learned how the skills and knowledge injection contributed to better overall security. The IT Department's prestige and reputation within the University has risen because agreed service levels are consistently met. The IT Executive set simple expectations for the IPsec relationship: assist the RMIT team to provide reliable and uniform security levels that protected stakeholder's privacy and the University's intellectual property. A complex security environment has been tamed and a better outcome delivered thanks to RMIT's partnership with IPsec.

Services

- Managed Security Service with industry leading 15 minute SLA
- Firewall and IPS configuration and a granular rules audit
- Network discovery and mapping
- Strategic and Operational Consulting

"IPsec provided RMIT with an injection of skills in addition to improving our response time when dealing with a high-severity security event"

Ben O'Neill

Deputy Director - ICT Infrastructure Delivery
RMIT University



About Us

IPsec specialise in protecting your information assets and mitigating security risks. Our team of highly skilled professionals design, implement, audit, and manage every aspect of your information security environment. By applying industry best practice to business processes, IPsec offer unrivalled service levels that protect your organisation and improves your overall security posture.

