

Kangaroo Bus Lines (KBL)

CASE STUDY



Sophos MDR (Managed Detect and Response)

What Was Done

Kangaroo Bus Lines partnered with Corp IT to implement the Guardian Security-as-a-Service solution — delivering enterprise-grade protection, greater resilience, and peace of mind. By refreshing aging infrastructure, integrating 24/7 Managed Detection and Response to Sophisticated Cyber Threats (MDR), introducing continuous vulnerability management, and empowering staff through human risk training, the Guardian Security-as-a-Service solution now enables KBL to operate with confidence, knowing their systems, data, and people are protected — without adding internal complexity. Working in close partnership with KBL's internal team, Corp IT ensured a seamless, secure transition that supports their ongoing growth and agility.

Overview of Customer

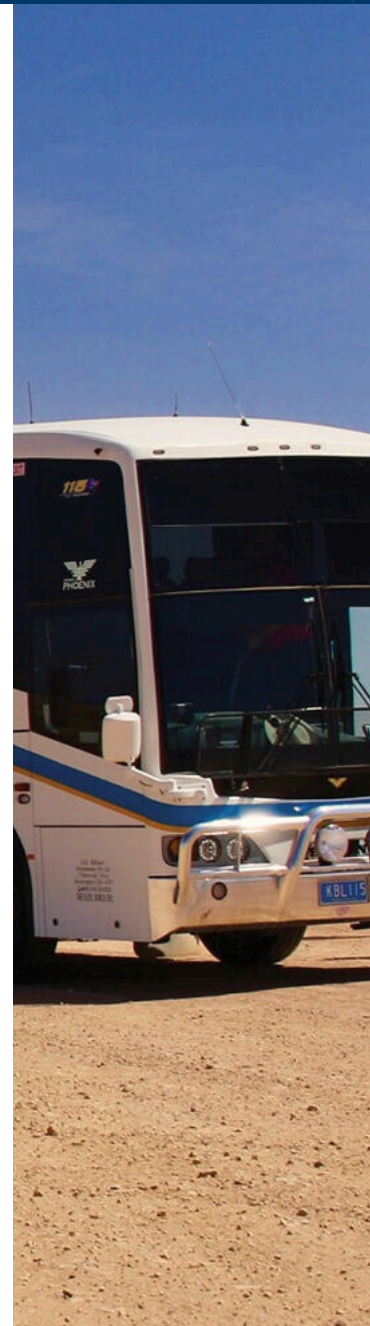
Kangaroo Bus Lines (KBL) is a family-owned transport provider based in Queensland, Australia, primarily servicing government-contracted school routes and public transport needs. With a proud history and reputation for service excellence, KBL has expanded significantly over recent years, growing their operational footprint and workforce. Their growth has seen a 25% increase in staffing over an 18 to 24-month period, alongside the opening of new operational sites. This rapid expansion placed additional pressure on their existing IT infrastructure and security systems, highlighting the need for a strategic technology refresh to support and safeguard their evolving business.

Challenge

KBL faced escalating cybersecurity risks as they expanded operations without adequate protection in place. Their infrastructure was aging, security posture was classified as high risk, and they lacked advanced protective measures. With ransomware threats on the rise and significant organizational growth underway, KBL needed to strengthen their cybersecurity posture to safeguard their assets and ensure sustainable growth and maintain trust with customers.

Customer Goals

KBL set out to strengthen their cybersecurity posture through proactive, organisation-wide measures that would ensure resilience against evolving threats. Their goals included fostering a strong culture of security awareness among staff, gaining greater visibility into system vulnerabilities, and protecting the business from emerging risks. Ultimately, KBL aimed to build a robust cybersecurity foundation to safeguard their people, assets, and reputation—creating a secure environment that would enable confident and sustainable growth.



Our Approach

Corp IT began by conducting a detailed review of KBL's current environment through a reinvigorated quarterly business review (QBR) process. This exercise, which had been neglected for nearly two years prior, provided a clear baseline of their existing posture and highlighted key areas for improvement. Working closely with KBL's leadership and internal technical team, Corp IT mapped out a customer journey that identified both immediate risks and long-term opportunities.

The solution involved refreshing critical hardware, including Sophos firewall devices, and deployed Sophos MDR (Manage Detect and Response), to deliver 24/7 threat hunting, monitoring, and proactive response to minimise sophisticated cyberattacks. In parallel, a Human Risk Management (HRM) solution was introduced to provide ongoing, automated cybersecurity awareness training for all staff, reducing risk by continuously improving employee vigilance and resilience. Additionally, a continuous vulnerability management system was put in place to scan KBL's entire IT network, giving real-time visibility into potential weaknesses and providing KBL with real-time insights to identify, prioritise, and address vulnerabilities—helping safeguard their business, maintain compliance, and confidently support ongoing growth.

Throughout the project, Corp IT maintained a strong customer-first approach, with a dedicated engineer managing approvals, change requests, and phased deployments to ensure transparency and trust. Regular feedback loops and customer satisfaction surveys confirmed the success of each implementation phase, reinforcing the strength of the partnership.

The Result

KBL's cybersecurity posture has significantly improved with the implementation of the Guardian Security-as-a-Service solution, drastically reducing their organizational risk. Their staff now benefit from Continuous cybersecurity awareness training becoming a frontline defense, improving internal resilience against evolving threats. Real-time continuous vulnerability monitoring has provided greater transparency and proactive risk management, ensuring issues are identified and addressed before they can impact operations. Corp IT's approach resulted in high levels of customer satisfaction, a strong relationship of trust. This partnership has positioned KBL with a robust, scalable security foundation — enabling them to confidently pursue ongoing expansion and operational success.

Deliverables

- Refreshed Aging IT infrastructure with modern security hardware
- 24/7 Sophos MDR (Managed Detection and Response) for sophisticated threat detection and response
- Continuous vulnerability management with real-time risk insights
- Human risk management for staff security training
- Security reviews to identify risks and opportunities
- Project management and phased implementation with ongoing QBRs
- Secure, seamless transition supporting rapid business growth
- Resilient cybersecurity foundation enabling confident expansion and compliance

Customer Quote

"Partnering with Corp IT on our cybersecurity uplift has been transformational. Their structured approach, proactive support, and clear communication gave us peace of mind as our business continues to grow. We now feel confident that our systems and people are well-protected for the future."

— Kangaroo Bus Lines

