LevelBlue

CASE STUDY

MS Plus boosts security operations with LevelBlue and Microsoft Sentinel integration

MS Plus is a leading Australian not-for-profit that supports people living with multiple sclerosis and other neurological conditions. With more than 65 years of care across Victoria, New South Wales, Australian Capital Territory, and Tasmania, MS Plus delivers vital services including neuropsychology, employment support, and wellbeing programs, all underpinned with a deep commitment to the privacy and security of those they serve.

As MS Plus expanded its use of client management systems and mobile access to sensitive data, it found itself requiring a scalable, integrated security framework to ensure protection and compliance in a complex healthcare environment.

The challenge

The organization faced growing regulatory pressure, with frameworks such as ISO 27001 and the Australian Privacy Principles mandating strong data governance, along with an increased cyber risk. MS Plus is supported by a lean in-house IT team, which found itself requiring enhanced threat visibility, faster response times, and access to specialized cyber expertise to deal with modern sophisticated threats.

The healthcare facility had previously invested in Microsoft 365 and Azure and now sought to consolidate and grow its security program through a closer alignment with Microsoft's cloud-native security ecosystem.

The solution

MS Plus partnered with LevelBlue to uplift its cyber defense posture and begin transitioning to a Microsoft-centric security architecture. LevelBlue supported the rollout of Microsoft Defender for Endpoint and Microsoft Sentinel, integrating its Co-Managed SOC model to deliver:

- Aggregation and enrichment of security telemetry across Microsoft and non-Microsoft platforms
- 24×7 monitoring and expert-led alert triage via LevelBlue's global Security Operations Center
- Context-rich threat intelligence and early detection of anomalous activity

LevelBlue worked in close collaboration with MS Plus' internal teams and Microsoft stakeholders to ensure seamless migration, while embedding best practices that optimized Sentinel's capabilities from day one.

The result

"With LevelBlue's support, we've taken a major step forward in our cyber maturity. The combination of Microsoft's tools and LevelBlue's expertise gives us clarity, speed, and confidence that we're protecting what matters most – our clients."

Peter Opie, CISO, MS Plus

Key benefits realized so far:

- Centralized visibility across clouds, endpoints, and application layers via Microsoft Sentinel
- A significant reduction in internal overhead for threat detection and response
- Improved alignment with regulatory and stakeholder expectations in healthcare and government
- Increased trust at the executive and board level in the organization's cyber resilience roadmap

What's next

The next phase of MS Plus's cybersecurity journey saw the implementation of LevelBlue's Managed Extended Detection and Response (MXDR) service for Microsoft Defender XDR and Sentinel. Here LevelBlue provides support and response actions natively in these tools. This will provide MS Plus with 24×7 extended threat detection, investigation, and response – leveraging automation and expert support to stop threats early, before damage is done.

As part of this uplift, LevelBlue implemented Response Authorization Protocol, which are client-defined response actions that ensure consistent communication and prioritization in high-pressure scenarios.

Because LevelBlue's security operations are directly connected to Microsoft's tools, LevelBlue can take swift action when something suspicious is detected, helping MS Plus respond faster, reduce risk, and keep their environment safe without overloading internal teams.

By choosing a partner who understands Microsoft security technologies and the mission-driven context of healthcare, MS Plus has built a future-ready cyber foundation. LevelBlue continues to support MS Plus with expert guidance, SOC capability, and Microsoft-aligned solutions that scale with the organization's needs, ensuring care delivery remains secure, resilient, and uninterrupted.