Identifies and remediates thousands of previously unknown threats.

**Healthcare organizations** are the most targeted by attackers

**Missed malware detected** on 50% of systems

**Prevention saves hours of time** for frontline IT staff

**Challenges**

- Healthcare organizations are the most targeted by attackers
- **IT team is spread thin across the 31 locations** from Sydney to the Queensland and Victoria borders
- **System downs** take away from nurses’ productivity
- **Email phishing** became a frequent problem for staff

**Reasons for Choosing Malwarebytes**

- **Data:** IT teams are able to see trends across systems and how many of the same attacks that succeed.
- **Automatic remediation:** Malwarebytes Linking Remediation Engine automatically remediates artifacts on systems that had been missed.
- **Cloud-based:** IT teams don’t have to manage an onsite server, saving travel time for the employees.

**How Malwarebytes Solved the Problem**

- **Identifies and remediates** thousands of previously unknown threats
- **Saves days of time** for IT team to focus on critical support activities
- **Stops malware and prevents infections** from proliferating
The ability to lock a machine off the network straight away when you identify an issue is fantastic. Just pushing a button to roll a system back is absolutely brilliant. It’s a phenomenal piece of technology.

Phil Sand, Senior Infrastructure Engineer
Southern Cross Care