CASE STUDY

Lack of visibility and endpoint protection puts school at risk of infection

1,400 devices were connected to the school’s network

Lack of visibility made it hard to gauge security of the system

Malwarebytes’ endpoint protection able to detect high volumes of infections

Challenges

- **Zero-day threats** were able to beat their old antivirus system
- **Lack of visibility** into the security status of the systems
- **Difficult to know** if a machine was infected or if a threat was lurking undetected
- **Off-campus computers** were at a higher risk

Reasons for Choosing Malwarebytes

- **Cloud-based solution**: Malwarebytes’ cloud-based management system allows the IT team to see and remediate all endpoints, regardless of where they are physically located
- **Widespread coverage**: Malwarebytes is able to cover both campuses in the McAuley College school system under one, unified system.
- **Small footprint**: Malwarebytes functions almost invisibly in the background, so systems run at their normal pace without being slowed down.

How Malwarebytes Solved the Problem

- **Extended coverage** easily for installed base computers with single site license
- **24/7 visibility** across all endpoints to ensures system and data defense
- **Enhances firewall performance** by using insight reports
Malwarebytes gives tremendous confidence because we have visibility across our entire fleet. We know we are protected.

David Mitchell, ICT Coordinator, Catherine McAuley College