Undetected malware threatens to disrupt company networks

Antivirus was not catching ransomware coming in via external devices

Issues solved with a quality and cost effective product

Hundreds of endpoints now easily managed

Challenges

- **Domino effect** occurred when one component of the network was infected or malfunctions
- **No way to know about existence** of all malware entering the network
- **Lurking threats** were still entering the system, even after cleaning up infections
- **Threats on endpoints** were not being caught by the previous antivirus system

Reasons for Choosing Malwarebytes

- **Cloud-based management**: Malwarebytes’ cloud-based console allows network access from the office and on the road.
- **Effective and cost-efficient**: Malwarebytes was able to provide a high-quality product for a price that fit into the company’s budget.
- **High-level threat analysis**: Malwarebytes notifies admin with a report regarding the types of malware targeting the company, allowing them to quickly initiate remediation measures.
- **Removes related artifacts**: Malwarebytes removes all threat artifacts linked to malware, so the IT team does not have to worry about any missed threats.
How Malwarebytes Solved the Problem

- **Prevents recurrence** of ransomware, eliminating associated downtime and disruption
- **Increased visibility** into current threat landscape and potential attack spikes
- **Simple endpoint protection management** across geographically distributed systems
- **Effective protection** with assurance of all threat artifacts being removed

We chose the right solution. We replaced our previous antivirus in weeks. Ransomware attacks are enormously disruptive, and with Malwarebytes blocking attacks, the business is happy, because it's business as usual.

Marcus Lee, Manager, Group Information Technology
Woodlands Transport Security Pte Ltd.