Faulty AVG server easily corrupted, allowing ransomware into network

Challenges

- **Malware was successfully evading** the current AVG antivirus solutions
- **Software updates were inconsistent** across servers, leaving some workstations without updated protection
- **Antivirus products would misidentify** updated applications as threats
- **AVG server was prone to corruption**, forcing the IT team to completely reinstall the software

Reasons for Choosing Malwarebytes

- **Multi-stage attack protection**: Malwarebytes combines advanced malware detection and remediation technologies, stopping attackers at every step.
- **Malicious website detection**: Malwarebytes identifies dangerous websites and malicious IP addresses and notifies the IT team.
- **Automated policy application and remediation capabilities**: Malwarebytes automatically quarantines detected threats, relieving the IT team from having to do everything manually as they did in the past with AVG.

How Malwarebytes Solved the Problem

- **Prevents future ransomware attacks** and removes artifacts from previous attacks
- **Stops attacks** on servers from malicious IP addresses
- **Simplifies endpoint security administration** with automated remediation and policy application
Malwarebytes’ effectiveness and ease of use have been a revelation. I don’t have to investigate every threat or install the software on new systems. Malwarebytes does it all and protects everything straightaway.

Rhys Wolloghan, IT Manager
Canterbury League Club