Weak antivirus systems leave remote devices vulnerable to threats

**Challenges**

- **Highly mobile workforce** makes it hard for company to protect endpoints
- **Antivirus solutions** were missing cyberthreats that infected mobile laptops and in-house systems
- **Impossible to ensure** that mobile endpoints had the latest protection
- **Increasing amounts of malware**, trojans, viruses, ransomware, and bitcoin mining threats were consuming computer-processing resources
- **Incidents would disrupt project work** and they could not afford to be down

**Reasons for Choosing Malwarebytes**

- **Layered protection**: Malwarebytes uses multiple technology layers to address advanced threats that leverage different attack vectors and techniques.
- **Powerful detection**: Malwarebytes Endpoint Protection blocks malware, phishing emails, and access to malicious websites while finding threats that other antivirus solutions miss.
- **Easy deployment**: Malwarebytes’ deployment tools simplify the process so that the program can be rolled out quickly.
- **Cloud console**: Malwarebytes’ cloud console ensures that all systems not connected to the network have updated protection.
How Malwarebytes Solved the Problem

- **Stops a wide range of threats** that other solutions miss
- **Verifies that all systems have the latest protection** even when not connected to the corporate network
- **Avoids hours of user downtime** and IT time spent remediating systems
- **Wide visibility** ensures that everyone is covered and greatly reduces the company’s attack surface