CASE STUDY

Poor antivirus system stealing productive hours from IT team

Challenges

- **Infections were entering** the Chart Industries Network via mobile endpoints and USB sticks
- **Most threats** had to be treated by re-imaging the infected machine
- **Hundreds of hours** were being taken away from strategic projects in order to re-image infected machines
- **Antivirus upgrades** did not deliver stable performance on the infrastructure or continuously report in real time

Reasons for Choosing Malwarebytes

- **Robust detection**: Malwarebytes Endpoint Protection covers the work of a multi-layered antivirus system on its own, eliminating the need for multiple systems.
- **Simplicity**: Replacing multiple systems with Malwarebytes simplifies the software management process and frees up storage on all devices.
- **Widespread deployment**: Malwarebytes is deployed from Chart’s primary data center, where it covers endpoints and user-facing data servers, including their email server.
The impact had been unbelievable. Malwarebytes has vaporized ransomware, and it runs silently unless it detects a serious threat that we need to investigate. It had been outstanding.

Kevin Merolla, Global IT Security Engineer, Chart Industries

How Malwarebytes Solved the Problem

- **Replaced Trend Micro** and stopped ransomware, malware, and inbound traffic from malicious sites
- **Reclaimed at least 200 hours** per month to focus on strategic security projects
- **Eliminated cost and management** associated with an ineffective antivirus
- **Catches threats** that get through the email filter and stops potential infections before they happen
- **Cleaned up traffic** on the publically-facing web servers by stopping traffic coming from malicious IP addresses