



The PC Security Channel

Stay Informed. Stay Secure.

Greenwich Place
London - UK

Malwarebytes EDR

Private Evaluation – Report

Executive Summary ([video playlist](#))

Malwarebytes EDR is a hassle-free experience for those with limited cybersecurity resources, allowing for a small staff to manage hundreds of endpoints with ease. The trade-off however is that it leaves the user entirely dependent on its own detection capabilities. Our experience suggests most IT admins will be able to handle all aspects of the Nebula UI, but analysts will struggle to investigate unknown processes or network activities unless they are flagged specifically. The product comes with a high level of automation and somewhat bridges the gap between typical anti-malware and analyst focused EDR solutions. The best parts about Malwarebytes EDR include a simplified incident handling process, low alerts, and great ransomware rollback capabilities.

Usability ([video](#))

- The user interface uses a simple two-layer approach that is geared towards admins rather than analysts
- Information about endpoints and detected threats is displayed concisely on the home screen
- Actions like remediating threats, isolating endpoints are easy to perform with essentially a single click
- Settings are highly customizable, although applying them to endpoints can be a multi-step process through groups and policies

-
- User groups and account management is fairly simple albeit a bit limited in terms of access customization
 - The product functions with a high level of automation and alerting is non-intrusive
 - This is one of the more silent EDR products we have tested
 - In our false positive test, Malwarebytes EDR performed above expectations and did not incorrectly flag any common files as false positives
 - While most of the user experience is coherent, it does not lend itself well to in depth investigations and search and analysis capabilities are not as powerful
 - Threat reports are easy to generate and the emails are great in terms of readability

Remediation ([video](#))

- Most remediation occurs automatically as the product detects and quarantines new threats in most cases
- In the event of suspicious activity, if enabled the feature can produce alerts for potential new threats or zero-day attacks
- Both a comprehensive lockdown and remediation can be carried out in a one click process that eliminates the complexity of incident handling
- Malwarebytes EDR features one of the best implementations we have seen of a simplified incident resolution process including ransomware rollback capabilities
- Due to the slow and reactive nature of the suspicious activity monitoring it may be susceptible to certain types of wipers like Petya and other less common threats like bootkits
- Malwarebytes EDR relies heavily on cloud sandbox analysis for most suspicious activity detections

Ransomware Rollback ([video](#))

- In a test against several contemporary and infamous ransomware including the likes of WastedLocker, BlackClaw, WannaCry and many others, Malwarebytes EDR was able to detect encryption behavior without the help of its signatures and perform a successful rollback

-
- While event detection took several minutes and the response was entirely reactive, in each case, all data was successfully restored
 - The rollback of user data is part of the remediation process and does not require any further action when configured correctly
 - Malwarebytes EDR provides a wide range of customization in terms of resource usage and rollback timeframe which can be configured up to several days, thus being one of the more flexible implementations of a rollback feature that we have encountered.
 - This feature, where applicable, is quiet and automatic, and provides good results with very little user intervention required

Threat Hunting ([video](#))

- Malwarebytes EDR provides basic threat hunting features through Flight Recorder and suspicious activity monitoring
- Several key metadata like process graphs and system activity logs are displayed in a clean, simplified, and user-friendly interface
- Event types (process/registry/network) are color coded and easy to identify
- Each suspicious activity is wrapped into an incident type view and presented with direct resolution options
- Integration with services like VirusTotal is quite limited and there are no avenues for in depth lookups of undetected processes
- Advanced search and investigation capabilities are limited, and the product cannot be used to perform any independent threat or event analysis
- There is a noted lack of sync between the Flight Recorder and suspicious activity views and switching between them can be tedious
- The product's threat hunting capabilities are focused on investigating incidents that are already detected and summarized and not unknown activity