SOLUTION BRIEF

Malwarebytes for Business

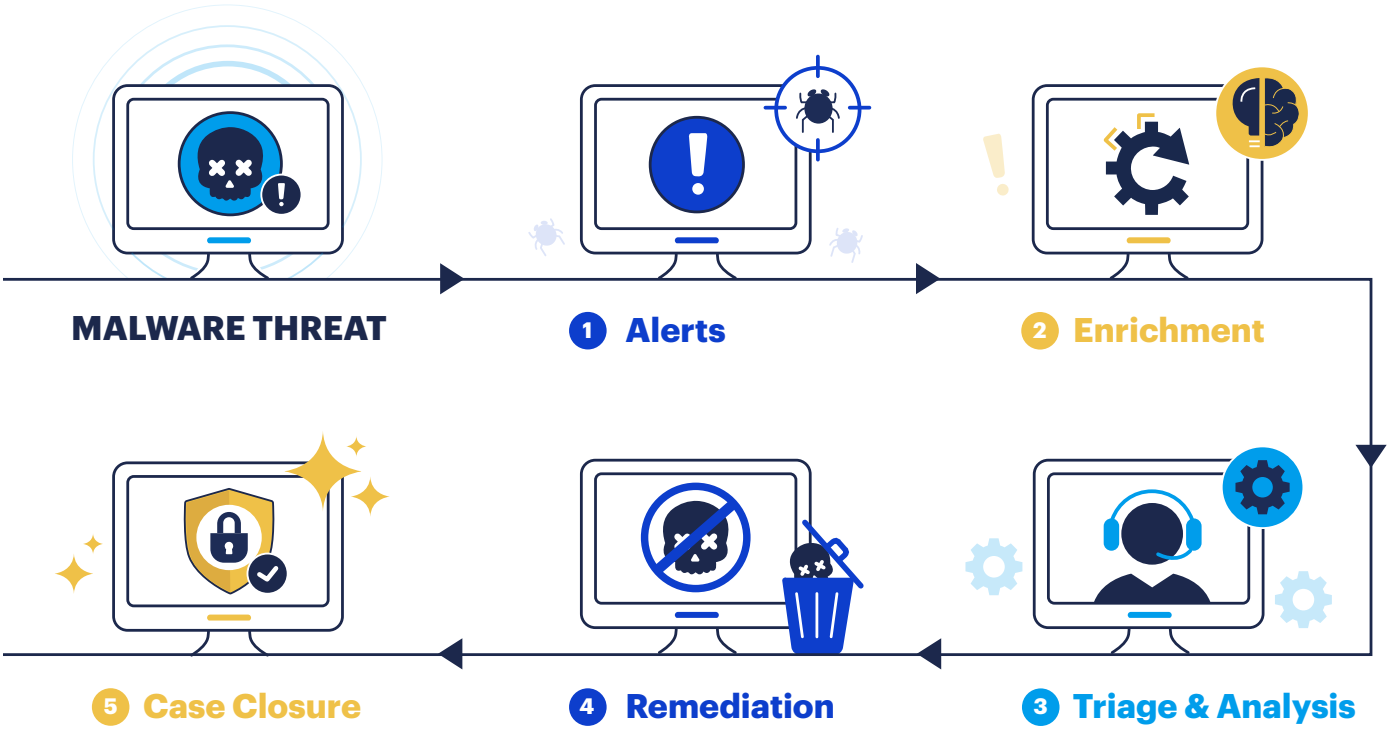
MALWAREBYTES MANAGED DETECTION AND RESPONSE (MDR)

Unlocking effective and fast threat detection and remediation

HOW IT WORKS

Malwarebytes MDR provides a powerful threat detection and remediation offering with 24x7x365 monitoring and investigations by our top-tier security analysts. Through a combination of powerful technology and top-notch security experts, your organization will gain a posture of cyber resilience with MDR services that accelerate threat detection and perform incident response with precision.

From initial threat alert to investigation closure, our experts are focused on delivering a high-quality service. The diagram below shows the process we follow to rapidly address threat alerts in your environment.



1 ALERTS

With Malwarebytes Endpoint Detection and Response (EDR) deployed in your environment, you'll gain a powerful first line of defense for threats to your organization. The solution is top ranked by third-party evaluations, including MITRE Engenuity Evaluations, MRG Effitas, and AV-TEST.org and includes seven layers of protection, multi-mode isolation, 72-hour ransomware rollback, and other comprehensive endpoint protection and detection capabilities.

Leveraging Malwarebytes EDR, our team of security experts provide 24x7 monitoring of your endpoints for threats to your organization. We'll consistently assess your EDR data to look for alerts that indicate suspicious activity, a detected threat, or an indicator of compromise (IOC).

2 ENRICHMENT

To obtain deeper analysis of your Malwarebytes EDR threat detections and the risk levels they pose to your organization, your EDR telemetry data is automatically ingested into our backend security orchestration, automation, and response (SOAR) platform. The SOAR platform also ingests threat intelligence feeds from multiple sources, which, collectively, provides correlated and contextual analysis of your EDR alerts.

This adds powerful SOAR capabilities to your security operations, maintained by our MDR team, and equips the MDR Analysts with additional information and insights about what is happening in your environment, enabling them to understand the threat and its potential impact quickly and easily. Armed with this information, your MDR Analysts can swiftly make informed decisions on the best course of action.

3 TRIAGE & ANALYSIS

Some MDR providers rely solely on their SOAR platform for analysis, which can create bias and lead to incorrect diagnosis. That's not the case with Malwarebytes MDR. Our backend SOAR automates menial tasks and correlation while our MDR Analysts provide the essential, hands-on analysis of threat behavior. They holistically investigate the telemetry context on your alert to efficiently assess if it's a real threat or a false positive.

Our approach provides a higher degree of accuracy and catches more threats, which includes the following steps:

- During the alert analysis, the MDR Analysts review specific artifacts to find those that require a deeper examination.
- A case is opened on each artifact that requires triage.
- MDR Analysts work together to look at all angles of the threat and define the best course of action.
- All steps and decisions made by MDR Analysts are tracked in the MDR Portal, keeping customers informed every step of the way.

4 REMEDIATION

When an alert is confirmed as a threat, the race is on to contain and remediate it. We understand that changes can occur on your security team, so you have the flexibility to choose the remediation approach that best supports your organization and needs. You can decide how response should be applied to your endpoints with the following options:

- **Malwarebytes managed:** The MDR Analysts remediate the threat on your behalf, informing your team of all the actions taken on your endpoints.
- **Customer managed:** The MDR Analysts provide guidance on recommended actions that your team can take to effectively remediate the threat.

5 CASE CLOSURE

Once the threat is remediated, we'll close the case and include granular documentation on the security events from the SOAR platform and our analysis. This information is preserved in the MDR Portal and made available for you to access for reporting, making it easy to reference for your governance, compliance, and other needs.

LEARN MORE

To learn more about how Malwarebytes MDR can help your business, visit: www.malwarebytes.com/mdr

malwarebytes.com/mdr corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes believes that when people and organizations are free from threats, they are free to thrive. Much more than malware remediations, the company provides cyberprotection, privacy, and prevention to tens of thousands of consumers and organizations every day. For more information, visit https://www.malwarebytes.com.