DATA SHEET

Malwarebytes and Rapid7 InsightIDR

Creating security efficiencies with leading endpoint protection and enriched SIEM analytics.

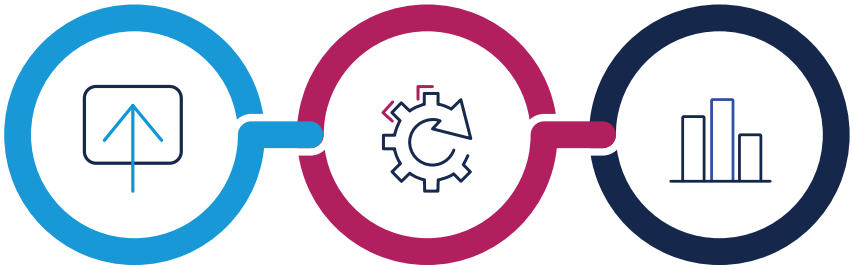
ABOUT RAPID7

Rapid7 is a cybersecurity company that offers a range of services and solutions that enable security teams to easily manage vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, or automate operations. Their flagship product, Rapid7 InsightIDR, is a cloud-native SIEM that accelerates detection and response for security teams.

Integration overview

The Malwarebytes integration with Rapid7 provides enriched intelligence that enables you to streamline threat investigations. This integration enables Malwarebytes alerts to be correlated with Rapid7 InsightIDR monitoring and analysis capabilities. By leveraging analytics on user behavior, network traffic, attacker behavior, and more, you gain greater content on the Malwarebytes alerts, enabling faster threat detection and response.

Capabilities



Secure syslog integration
Our pre-built syslog integration enables you to easily connect the Malwarebytes Nebula platform to Rapid7 InsightIDR, enabling seamless setup out-of-the-box.

- Install Rapid7 Collector component on Windows Server or Linux Server machine
- Easily configure secure syslog connection in Malwarebytes Nebula console

Automated event sharing
With a simple configuration in your Rapid7 InsightIDR console, you can enable the Malwarebytes Nebula events to be forwarded from the Collector and ingested for analysis.

- Automatically sends specified Malwarebytes endpoints events to the Windows or Linux Collector
- Rapid7 Collector forwards events to InsightIDR where they are available for analysis

Correlation and analysis
InsightIDR correlation of user behavior data, network traffic, attacker behavior, and other analytic features along with new context from Malwarebytes alerts provide deeper insights and empower you to make faster investigation decisions.

- Create a more complete picture of your security posture with security alerts from multiple data sources correlated within InsightIDR
- Respond more efficiently and rapidly to threats with added context

LEARN MORE

To learn more about the Malwarebytes and Rapid7 integration, visit: www.malwarebytes.com/integrations

malwarebytes.com/business 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 remediation, 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.