DATA SHEET

Malwarebytes and QRadar

Simplifying threat investigations and response on your endpoints

ABOUT QRADAR

QRadar is a SIEM platform that helps security teams accurately detect and prioritize threats across the enterprise, and it provides intelligent insights that enable teams to respond quickly to reduce the impact of incidents.

By consolidating log events and network flow data from thousands of devices, endpoints and applications distributed throughout your network, QRadar correlates all this different information and aggregates related events into single alerts to accelerates incident analysis and remediation.

Integration overview

The Malwarebytes integration with the QRadar SIEM platform enriches QRadar's threat analytics with endpoint alerts correlated with log events and network flow, providing greater context and simplifying your organization's threat investigations.

The integration also enables security teams to automate deployment of the agentless version of Malwarebytes Incident Response to automate malware removal when QRadar alerts on a security incident that requires rapid remediation.

Capabilities

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

- Easily configure secure syslog connection in Malwarebytes Nebula console

Secure syslog integration

Correlation and analysis

Automated endpoint remediation

Correlation and analysis
By correlating log events and network traffic data with data from fleets of endpoints, QRadar aggregates related events into single, meaningful alerts to accelerate threat investigations and remediation.

- Security alerts from Malwarebytes endpoints and other data sources are correlated by QRadar, providing security teams with a more complete picture of gaps in the security perimeter
- New context on Malwarebytes endpoint alerts empowers teams respond more efficiently and rapidly to threats.

Automated endpoint remediation
When QRadar has identifies a threat on an endpoint, the SIEM platform triggers the deployment of the Malwarebytes Incident Response agent to endpoints, which performs an automated endpoint scan and completed remediation of identified malware threats.

- The Malwarebytes IR agent is deployed, as needed, when you have a detected threat to eradicate
- After remediation is complete, you can harvest the logs for reporting and delete (i.e., dissolve) the agent and files

LEARN MORE

To learn more about the Malwarebytes and QRadar 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/.

Copyright © 2021, Malwarebytes. All rights reserved. Malwarebytes and the Malwarebytes logo are trademarks of Malwarebytes. Other marks and brands may be claimed as the property of others. All descriptions and specifications herein are subject to change without notice and are provided without warranty of any kind.