Malwarebytes

SOLUTION BRIEF

SIEM integrations to enrich threat intelligence

Running security operations requires situational awareness—one where your security analysts have a complete picture of the organization's security posture across disparate parts of the network. This requires bridging data silos so that your team can work from a single pane of glass.

Malwarebytes Business Products help you achieve this goal by providing integration opportunities with multiple security information and event management (SIEM) platforms. This supports your security team with several use cases that enrich your threat intelligence to drive efficient investigations and response actions.

Use Case: Correlate security data

When your security team correlates endpoint security data with other security data, such as information from the network, they gain a more complete picture of vulnerabilities. Siloed data can't offer an accurate picture of weak and vulnerable areas of internal systems. Correlated security data helps establish relationships between data sources, enabling you to make more informed decisions on how to protect against threats.

Example of how Malwarebytes and SIEM integration helps verify security incidents from multiple data sources:

- Data from multiple security-related tools, such as network monitoring, firewall management, and endpoint security is ingested into a SIEM platform
- An analyst sees a network traffic spike from a known threat actor IP address
- Concerned about possible malware delivery on end-user machines, an analyst timeboxes the traffic event across all data sources
- The analyst monitors data from a single pane of glass, looking for anomalous or nefarious behavior indicating a security breach
- Across Malwarebytes and the other data sources, no evidence of a breach is found. It is determined that the network traffic spike event is not connected to a security incident.

Security operations benefits:
Assembling all the pieces is powerful. In a network environment, thousands of security events and bits of information are generated daily. Manual correlation is nearly impossible with today's data volumes. Data correlation helps determine relationships between events and sources of cyberthreats that, in turn, enable you to take better actions and decisions.

The data is not only beneficial for risk mitigation, but also for operations and organizational considerations. Data correlation offers a "big picture" view that can help security leaders acquire information about where to invest in resources, as well as determine where time may be better spent by team members.

Malwarebytes Partner integrations that support this use case:
IBM QRadar, Rapid7, Azure Sentinel, Splunk

Use Case: Magnify visualization of security data

Visualization brings security data from varying sources together in a cohesive way, offering a different perspective for decision-making. Your security team can view information faster and more easily with graphs that identify recurring patterns, or a process diagram that shows the severity of an incident.

Through integrations with Malwarebytes, you can “double-click” to magnify their view of security data. You can integrate endpoint data into other IT security data sources and leverage those capabilities to visualize data, understand attack vectors, and make better security decisions in the future.

How Malwarebytes integration assists with visualizing network spread of a cyberthreat:

- Data from multiple security-related tools, such as network monitoring, firewall management, endpoint security, and server data is integrated with a SIEM solution
- Malwarebytes Suspicious Activity alerts of a newly discovered incident on both servers and workstations, denoting possible ransomware activity via the SIEM platform, an analyst sends Malwarebytes an action to isolate and remediate the attack, including conducting a ransomware rollback
- Analysts use the log data and other security data received in the SIEM platform to trace the malware spread back to additional endpoints and servers, which are possibly compromised
- Malwarebytes conducts a systemwide scan and isolates and remediates the attack spread, restoring the infected endpoints to a clean state

Security operations benefits:
With data visualization, you don’t just talk about potential malicious activity—you see it. The graphic representations of patterns and behaviors provide a fresh perspective on data to improve decision-making.

Malwarebytes Partner integrations that support this use case:
Azure Sentinel, Splunk, IBM QRadar, Rapid7

LEARN MORE

Want to learn more about our integrations?

Visit 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.