Malwarebytes and Splunk Phantom

Endpoint security integrated for enterprise resilience

Malwarebytes’ Endpoint Protection and Incident Response cloud integration with Splunk Phantom automates and orchestrates cyberthreat protection and responses across the enterprise. With this bidirectional integration, security teams can prevent, detect, and remediate infected endpoints faster without impacting end-user productivity.

Integration benefits

Simplify complex response policies
Splunk Phantom integrates with Malwarebytes endpoint intelligence and orchestrates responses and processes through playbooks. These customizable playbooks can execute automated responses across your IT infrastructure.

Automate endpoint security actions
Reduce manual tasks and save valuable IT staff resources by automating Malwarebytes protection and responses with Splunk Phantom “actions” that orchestrates Malwarebytes’ API.

Comprehensive threat intelligence
Add endpoint intelligence to Phantom and programmatically or manually query comprehensive threat intelligence for better decision making.

Malwarebytes provides the leading endpoint security solution that delivers enterprise resilience to ensure workforce productivity.

Adaptive cyber protection
Layered protection, including machine learning and behavior analytics, anti-exploit, and ransomware mitigation that adapts to the type of attacks.

Active threat response
Automatically quarantine and remediate malware and other threats centrally with proprietary Linking Engine technology that removes all threat artifacts completely.

Orchestrated endpoint control
Cloud extensibility and API-delivered integration provide threat response automation through your existing SIEM and ITSM tools.
Integration use cases (Bidirectional integration)

**1. Send data to Playbooks**
- **Malwarebytes** Send security telemetry and associated asset data
- **Splunk Phantom** Receive and act in Phantom playbooks

**2. Automate actions**
- **Malwarebytes** Automate remediation (quarantine, remove)
- **Splunk Phantom** Receive detection notification

**3. Detect, Review, Scan All**
- **Malwarebytes** Detect and remediate or just remediate
- **Splunk Phantom** Integrate into Phantom actions