Malwarebytes and Splunk Enterprise Security
Endpoint security integrated for enterprise resilience

Malwarebytes' endpoint security bidirectional integration (Incident Response, Endpoint Protection, and Endpoint Protection and Response), which is compatible with Splunk Enterprise Security, and Splunk Cloud, provides comprehensive threat hunting and analysis across the enterprise. Security teams can consolidate and analyze threat data, and automate remediation of infected endpoints faster without impacting end-user productivity.

**Integration benefits**

**Agentless breach remediation**
Automate responses with non-presistent agents that scan and remove malware across networked endpoints.

**Automated endpoint security actions**
Reduce manual tasks and dwell time by automating Malwarebytes protection and response within Splunk.

**Comprehensive threat intelligence**
Add Malwarebytes endpoint intelligence to Splunk Enterprise Security dashboards for comprehensive threat intelligence and 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. **Correlate and analyze data**
   - Send security telemetry and associated asset data
   - Analyze endpoint data with other data sources in Splunk Enterprise/Cloud
   - Receive detection notification

2. **Automate actions**
   - Automate remediation (scan, quarantine, remove)
1. Malwarebytes Visibility and Dashboards
Provides pre-built dashboards of security and operational insights from Malwarebytes protected endpoints
- High level operational overviews
- Endpoint activity, agent distribution and insights
- Endpoint threat activity and insights
- Near real-time visibility
- Operational dashboard customization

2. Malwarebytes Agentless Remediation
Use Splunk Enterprise Security workflows and alert action add-ons to automate Malwarebytes endpoint breach remediation on-premises solution
- Deploy non-presistent agent centrally from Splunk
- Proprietary Linking Engine technology assures complete removal of threat artifacts

3. Malwarebytes Cloud Remediation
API integration with Malwarebytes cloud platform, including incident Response, Endpoint Protection, and Endpoint Protection and Response products
- Protect, detect, quarantine, and remove threats
- Automate scan and remove all threat artifacts
- Search, monitor, and report on endpoints

4. Technical Add-on
Converts Malwarebytes' data to Splunk CIM format to ensure Malwarebytes is a compliant data source. Allows all data from Malwarebytes to be consumable in Splunk apps.

Next Steps
Download free apps here and start realizing their benefits. malwarebytes.com/integrations.