Malwarebytes

SOLUTION BRIEF

SOAR integrations to streamline endpoint security

When enterprises automate the orchestration of integrated endpoint security tasks between their complex, distributed security ecosystems and services, they streamline, accelerate, and simplify security processes and operations. Malwarebytes has several key integrations that help automate some of the most critical responsibilities in a security operations center.

Malwarebytes Business Products help you achieve this goal by providing integration opportunities with multiple security orchestration, automation and response (SOAR) platforms. This supports your security team with several use cases that enrich your security orchestration to drive nimble and effective processes.

Use case: Automate endpoint scanning and isolation

One of the most critical responsibilities of the security team is to regularly scan endpoints to identify and uncover threats and infections. This is a highly repetitive process that must occur, so why not automate it?

Through integrations with Malwarebytes, automated endpoint scans from pre-scheduled events can take place, service tickets are automatically input into a SOAR platform, threat discovery is immediate, and isolation takes place quickly to impede lateral spread.

Example of how Malwarebytes helps automate endpoint scanning:

- Data from multiple security-related tools are integrated onto a SOAR platform
- A SOAR platform identifies an incident and automatically sends Malwarebytes an action to isolate the endpoint to stop any lateral spread
- SOAR playbooks initiate Malwarebytes to conduct an endpoint scan and remediation. The scan positively identifies the piece of malware on the machine and updates the support ticket with this information.
- Malwarebytes remediation occurs, successful removal of malware is confirmed, and the support ticket is automatically updated with this information on a SOAR platform
- A SOAR platform updates the incident and a security analyst is notified of the events. The analyst can perform additional actions to remove isolation on the endpoint, if required.

Security operations benefits:
Automating endpoint scans reduces response time, minimizes threat dwell time and impact, and eliminates the hands-on process required if teams scan manually. By automating this critical process, security systems can regularly detect anomalies or other nefarious activity.

Malwarebytes Partner integrations that support this use case:
ServiceNow, Splunk Phantom, Cortex XSOAR, ForeScout

Use case: Orchestrate security software installation

In environments where security and IT teams work separately, software installation is sometimes a challenge. If IT owns the endpoint, for example, it is often necessary to obtain their assistance with certain installations. With Malwarebytes integration, however, security teams can skip this manual, time-consuming process if a security problem is identified on an endpoint.

How Malwarebytes integration expedites an endpoint security software installation and scan:

- User submits support ticket, reporting excessive pop-up windows and other nuisance activities
- A ticket is logged in a SOAR platform and reviewed by a security analyst
- The analyst classifies the issue as malware, and initiates Malwarebytes Incident Response (IR) through a SOAR platform
- A SOAR platform automatically copies the IR package on the user machine. IR scans the endpoint, sends back positive identification of malware, and then remediates the malware.
- Successful remediation is reported by IR and the support ticket is updated
- IR deletes itself (i.e., dissolves) the agent and files from the user machine, and the problem is resolved

Security operations benefits:
When a threat is detected, teams can execute a scan, perform remediation, and remove the software, without jumping through hoops. This integration eliminates the manual processes for distributing security software, removing time-consuming steps to coordinate between separate security and IT departments.

Malwarebytes Partner integrations that support this use case:
BigFix, Microsoft SCCM, Forescout, Splunk Phantom, ServiceNow

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.