Malwarebytes™

Malwarebytes and Microsoft System Center Configuration Manager

Orchestrate security software installation for fast endpoint remediation

About Microsoft SCCM

The Microsoft System Center Configuration Manager is an administration tool that enables organizations to manage and safeguard devices and software within its environment. SCCM takes care of the hardware inventory, distributing software and patches, and more. SCCM is now part of the Microsoft Endpoint Manager platform and widely used across IT departments worldwide.

Integration overview

The integration with Microsoft System Center Configuration Manager (Microsoft SCCM) makes it easy to deploy Malwarebytes to your endpoints. The integration also enables security teams to automate deployment of the agentless version of Malwarebytes Incident Response (Malwarebytes IR), which automates malware removal when you detect a security incident that requires rapid remediation.

Capabilities

Automate endpoint remediation

Orchestrate software installation

Automated log collection

Automate endpoint remediation

When your security controls detect a threat on an endpoint, Microsoft SCCM can trigger the deployment of the Malwarebytes Incident Response agent to endpoints, which performs an automated endpoint scan and completes 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

Orchestrate software installation

In environments where security and IT teams work separately, software installation is sometimes a challenge. The Malwarebytes IR and Microsoft SCCM integration scripts let you deploy, register, and update Microsoft IR to Windows endpoints

- Deploy, register, and update Malwarebytes IR to your Windows endpoints
- The Malwarebytes scripts must be installed and configured on your Microsoft SCCM platform

Automated log collection

The pre-built log collection script for Microsoft SCCM makes it simple to capture the Malwarebytes IR data from your endpoint scans and send them to your syslog server for further forensic analysis or annotating to your incident ticket.

- Collect Malwarebytes scan data and send to your syslog server
- To enrich your threat intelligence, you can use the syslog protocol to send your logs to your SIEM solution

Requirements

- Malwarebytes Nebula
- Malwarebytes Incident Response (IR)

LEARN MORE

To learn more about the Malwarebytes and Microsoft SCCM 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.