Introduction to Azure VM endpoint protection

Microsoft Antimalware



Samples reporting

troubleshooting.

Microsoft Antimalware for Azure is a free real-time protection that helps identify and remove viruses, spyware, and other malicious software. It generates alerts when known malicious or unwanted software tries to install itself or run on your Azure systems.

Antimalware

Features

Real time protection

Monitors activity in Cloud Services and on Virtual Machines to detect and block malware execution

Scheduled scanning

Scans periodically to detect malware, including actively running programs.

Malware remediation

Automatically takes action on detected malware, such as deleting or quarantining malicious files.

Signature updates

Automatically installs the latest protection signatures

Provides and reports samples to the Microsoft Antimalware service to help refine the service and enable

Antimalware event collection

Records the antimalware service health, suspicious activities, and remediation actions taken in the operating system event log

Exclusions

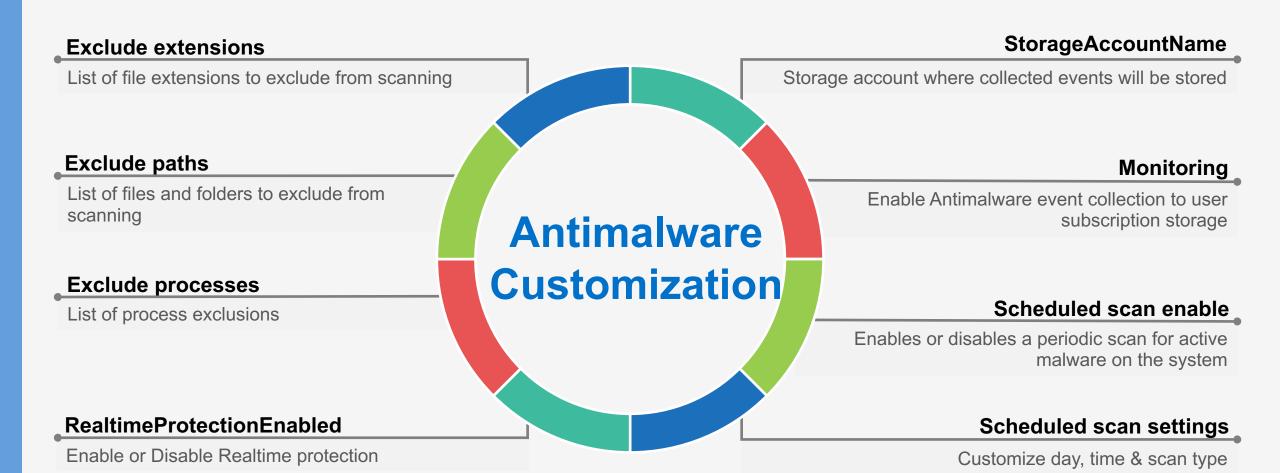
Allows application and service administrators to configure exclusions for files, processes, and drives

Antimalware engine and platform updates

Automatically updates Antimalware engine and platform

Antimalware customisation





Deployment scenarios





Virtual machines & Scale sets



Cloud services



App services

The Microsoft Antimalware Client and Service is not installed by default in the Virtual Machines platform

For virtual machines, install as an extension using Azure portal, Visual studio and Cmdlets The Microsoft Antimalware Client and Service is installed by default in a disabled state in all supported Azure guest operating system families in the Cloud Services platform

For cloud service, use AntiMalware PowerShell Cmdlets When using Azure App Service, the underlying service that hosts the web app has Microsoft Antimalware enabled on it.

Events written to System OS events log under the "Microsoft Antimalware"

