Barracuda Managed XDR

SentinelOne - 24.1 Windows Agent Release Notes

October 2, 2024

The purpose of this article is to outline the various improvements in the upcoming SentinelOne agent upgrade. The lists below do not include an exhaustive list of all release notes, but rather a summation of the most notable improvements.

Current Stable version: 23.4.4.22
Target Stable version: 24.1.4.257 GA
OS: Windows
This agent version and its new features have undergone extensive testing and validation by SentinelOne and have been further tested in a lab environment before being identified as stable by the Barracuda XDR Endpoint Security Team.

Upgrade Timeline

The new agent version, 24.1.4.257 GA (General Availability), which was marked GA on September 30, 2024. This agent upgrade will be pushed out in phases over the next 1-2 weeks across all Managed Endpoint Security partners. The upgrade process is silent, and no interruption, input, or reboot will be needed from our partners.

SentinelOne Agent Group Update

With the rollout of the new S1 agent version, we are also taking proactive steps to enhance partner Endpoint Security Posture. Third-party backup software, such as Veeam, can occasionally be impeded by the SentinelOne agent due to its built-in VSS and/or Safe Boot Protection. Thus, we will soon enable an automatic process that does the following, on a monthly basis:

1. Checks for any agents with the Veeam backup agent installed.
2. If the Veeam agent is present, a "Monitor + Remediation + Safe Boot Protection Disabled" group will be created in the site if one does not already exist.
3. Veeam exclusions will be implemented for the new group.
4. The agents with Veeam installed will be moved into the new group.

Contact the SOC if you have any questions.

Important – Agent Version Compatibility Changes

Windows Agents 24.1 and higher are compatible **only** with specific 64-bit Windows OS versions and is **not** compatible with 32-bit Windows OS versions.

Windows Agent 24.1 is compatible only with these Windows versions:

- Windows 8.1 64-bit
- Windows 10 64-bit
- Windows 11 64-bit
- Windows Server/Storage Server 2012 R2 64-bit

- Windows Server/Storage Server/Server Core 2016 64-bit
- Windows Server/Server Core 2019 64-bit
- Windows Server/Storage Server 2022 64-bit

Windows Agent version 24.1 is **not** supported on:

- Endpoints running 32-bit versions of Windows.
- Endpoints running 64-bit versions of Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8 (not 8.1), and Windows Server 2012 (not R2).
- Endpoints running these OS versions will remain on the latest supported agent build.

Support for ARM-based architecture: SentinelOne released a version of the Windows Agent compatible with endpoints that utilize ARM processors. The Windows Agent for ARM is installed like any other Windows Agent 22.1+ EXE. Contact the SOC if you need the ARM installer.

ARM Limitations:

- This package is only compatible on Windows 11 with an ARM processor.
- Some detection engines on ARM are expected to receive enhancements in a future version.
- Make sure to not have any previous installments of the Agent on the endpoint.

Detection Enhancements:

- The Driver Blocking engine now offers the kill action for drivers whose dropper, loader, and installer are part of the same Storyline™.
- The macro mitigation feature now fully mitigates all K4 macro modules.
- Improved detection of:
  - Jupyter Infostealer. New Behavioral Indicators were added.
  - Macro threats.
  - NetSupport Remote Access Trojan (RAT).
  - Nim Reverse Shell.
  - Wipers.

New AI detection and visibility:

Description	**Behavioral Indicator**
Detects when a process registered a custom extension to a malicious binary.	SuspiciousCustomExtensionToMaliciousBinary
Detects when a process registered a custom extension that spawns an interpreter with a command line.	SuspiciousCustomExtensionToInterpreter
Detects a first stage RedLine attack pattern.	RedlineAttackChain
Detects first stage IcedId attack pattern.	IcedIdAttackChain
Detects a Raspberry Robin attack pattern.	RaspberryRobinAttackChain
Detects a first stage SocGholish attack pattern.	SocgholishAttackChain

Description	Behavioral Indicator
Detects SocGholish proxy script.	SocGholishProxyServer
Detects possible DarkGate Loader AutoIt Execution.	PossibleDarkGateLoader
Detects extractions of files using a renamed 7z.exe process and a password protected archive.	RenamedArchiveExtraction
Detects a scheduled task created by PHP.	PhpTaskRegistered
Detects hook removal attempts by a known attack framework.	KnownAttackFrameworkHookRemovalAttempt
Detects threats that attempt to terminate protected threads for AV evasion.	AntiVirusEvasionTerminateThread
Detects threats that attempt to modify an EFI system partition file for AV evasion.	AntiVirusEvasionModifyEfiSystemPartitionFile

New AI indicators for analysis and threat hunting:

Description	Behavioral Indicator
Detects threats that attempt to modify an EFI system partition file for AV evasion.	AntiVirusEvasionModifyEfiSystemPartitionFileExtended
Detects when a Powershell stager is used.	PowershellStager
Detects DLLs with cloud file reparse points loaded into PPL processes.	CloudReparsePointDllLoadInPplProcess
Detects possible privilege escalation attack through impersonation through named pipes.	GenericFakePipeImpersonation LanmanImpersonation
Detects credential-stealing attempts from a fake Windows login window using the credui.dll API from a signed process.	SignedProcessCreatedCredentialPrompt
Detects credential-stealing attempts from a fake Windows login window using the credui.dll API from an unsigned process.	UnsignedProcessCreatedCredentialPrompt
Detects process calling of a kernel live-dump from Windows.	KernelLiveDump
Detects process calling of a kernel live-dump from the SentinelOne Agent.	KernelLiveDumpViaSentinel
Detects STD handle redirection to network connections.	CommandProcessorRedirectionToPipe
Detects STD handle redirection to network connections in a forbidden process.	CommandProcessorRedirectionToPipeInForbiddenSpawn

Description	Behavioral Indicator
Detects STD handle redirection to network connections in an interpreter with a command line.	CommandProcessorRedirectionToPipeInInterpreterWithCli
Detects STD handle redirection to network connections in an unknown binary.	CommandProcessorRedirectionToPipeInUnknownBinary
Detects Wiper activity based on general deletion.	WiperDeleteGeneralFiles
Detects when a process registered a custom extension to a forbidden process with a command line.	SuspiciousCustomExtensionWithCli
Detects when a non-PowerShell process loads a PowerShell assembly and executes a PowerShell script or command from memory.	PowershellDllLoadedAndReflectiveLoad

Bug Fixes:

- Interoperability issue with Veritas backup services.
- USB docks, and the USB peripherals connected to them, caused USB devices to disconnect.
- When the Windows Security Center service was disabled or stopped and Windows Defender was running, there were interoperability issues with Excel.
- Increased login time when the data directory for the Agent was located on a separate volume from the System volume.
- To solve performance issues, in Win 24.1 by default deep hooking is disabled on VMware machines with VBS enabled. Previously, it was enabled.

False Positive Fixes:

- Detection of Sophos.
- Detection on PowerShell.
- Detections on *poqexec.exe* when *TrustedInstaller.exe* tried to remove snapshots.
- Detections on DocuWare.
- Detections on Quest *SLAgent.exe*.
- Detection on Powershell installation or upgrade with *winget*.
- Static AI False-Positive detections sometimes caused files to be quarantined due to incorrect file caching.