SentinelOne - 25.1 Windows Agent Release Notes

August 12, 2025

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: 24.2.3.471 GA
Target Stable version: 25.1.3.334 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, 25.1.3.334 GA was declared GA by SentinelOne on August 12th, 2025.
This agent upgrade will be pushed out in phases over the next 2-6 weeks across all Managed Endpoint Security partners. The upgrade process is silent, and no interruption, input, or reboot will be needed from our partners.

Reminder – Agent Version Compatibility Changes as of 25.1

As a reminder, Windows Agents 25.1 and higher are compatible **only** with specific 64-bit Windows OS versions and are **not** compatible with all 32-bit Windows OS versions.

Windows Agent 25.1+ 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 25.1+ 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.

Barracuda Managed XDR™

Detection Enhancements:

- **Network monitoring infrastructure added**: Infrastructure has been added to the 25.1.2 Agent to lay the groundwork for future Agent network monitoring capabilities. This functionality tracks new connections and connection terminations. The capabilities that have been added are enabled by default but will not trigger any detections nor are expected to impact Agent performance.
- **Support for Windows 365**: From Agent version 25.1, you can run SentinelOne Agents on Windows 365, helping you achieve full protection and visibility over your Windows 365 environments.
- **Improved mitigation for malicious .NET applications**: The .NET protection infrastructure of the Agent now applies to all .NET processes. This infrastructure gives the Agent more visibility and mitigation capabilities against malicious .NET techniques exploited by .NET malware and tools.

Bug Fixes: Resolved Issues in Windows Agent 25.1

- Interoperability issue with WebAssembly applications in Microsoft Edge.
- Quarantined files were not properly decrypted when attempting to unquarantine them from one volume to a restoration target in a different volume.
- If the combined number of event IDs and levels exceeded 23 in a Windows event log collection policy override, logs would not be ingested.
- Agent performance issues with large LDAP queries.
- In multi-domain forests, failures to reach or resolve the primary domain controller during onboarding, updating Active Directory (AD) configuration, or scheduling AD assessments caused SMB exposure checks that rely on multiple domain controllers to be skipped.
- Interoperability issue with .NET support for .NET 9 and PowerShell version 7.5.0. These versions are now supported.
- The sentinelctl disable_agent command did not reboot the system after successfully disabling the Agent. The documentation also contained misinformation about the -r parameter.
- After a failed upgrade, commands sent to the Agent failed.
- Microsoft Entra ID information was sometimes not retrieved by the Agent.
- Interoperability issue with ThreatLocker.
- Interoperability issue with third-party boot drivers which caused inaccessible boot devices or failures to boot.
- The Citrix user profile took a long time to load for the first time.
- Interoperability issue with Citrix that caused performance issues.
- Detection of critical processes that cannot be mitigated led to unnecessary reboot requests.
- Some policy override configurations did not show after Agent reload or reboot.
- Certain deadlocks caused by interoperability with other security products resolved using new Windows 10 features.
- The sentinelctl disable_agent did not run as described in the documentation and triggered error messages.
- Login was sometimes slow on new endpoints when user logged in for the first time.
- Remediation did not always delete all files from a VSS NTDS harvesting technique.
- IP address of Lateral Movement shown as "Unknown Address" due to mishandling TCP events.

- When suppress alert exclusions are configured, the Agent pre-emptively blocks an event, but it also suppresses its threat.
- Multiple lateral movement unknown address detections.
- Upgrade sometimes failed with error 0x800706be due to failure to disable Antitampering.
- An issue in the Agent's internal file system tracking caused issues with quarantine in some cases.
- An interoperability issue with the Rapid7 vulnerability scanner.
- Improved Agent performance during Windows updates.
- Threats detected immediately after being downloaded with Chrome showed only a partial filename.
- Fixed a bug in PowershellStagerArtifacts.
- A signed PowerShell script showed as unsigned in the Console and in Agent logs. The Agent checks these file types for digital signatures:
  - Portable executables, which are files that start with the letters "MZ" and the numbers 4D 5A in hexadecimal.
  - Files with the extensions: EXE, SCR, DLL, SYS, COM, MSI, MUI, MSP, JAR, OCX, CPL, DRV, EFI, TSP, ACM, AX, XLL, SDB.

False Positive Fixes:

- Behavioral detections on MultipleInfostealers.
- Behavioral detections on SuspiciousRegistrySessionManagerExecutePersistence.
- Behavioral detections on ShadowCopyDeletion.
- Behavioral detections on Ransomware.
- Behavioral detections on SuspiciousInjectionToBrowser.
- Behavioral detections on CredsReadFromLsass.
- Renamed behavioral indicator SuspiciousProcessCreation to SuspiciousSvchostProcessCreation.
- Detections on Rapid7 from SuspiciousInjection and SuspiciousInjectionToBrowser.
- Detections on PowerShell Get-ADGroupMember and Get-ADDomain commands.
- Ransomware detections on jQWidgets-related files.
- Alerts on McAfee WebAdvisor.
- Detection on rpcnetp.exe.

New AI detection and visibility:

Description	Behavioral Indicator
Detects obfuscated interpreter created by an mshta process with a downloaded file.	ObfuscatedInterpreterFromMshtaDownloadedFile
Detects execution of Gladinet CentreStack exploits process chain (CVE-2025-30406).	GladinetExploitPayloadProcessChain
Detected attempt to query the SAM.	QuerySAM

Barracuda
Managed XDR™

Description	Behavioral Indicator
Detects a hook bypass attempt using breakpoints without a debugger attached to a lolbin process.	BreakpointHookBypassWithoutDebuggerFromLolbins
Detects suspicious unknown Rclone capability abuse.	UnknownRcloneDataExfil
Process dumped local machine hive	DumpLocalMachineHive
Suspicious AsyncRat Process Chain	AsyncRatWscriptProcessChain
A POWERTRASH powershell script executed	A POWERTRASH powershell script executed
Detects execution of PowerShell through Microsoft SQL Server (SQL injection exploitation)	SqlServerPowershellExecution
Detects a process tree pattern that matches gootloader	GootLoaderProcessChain
Suspicious Rclone abuse for exfiltration	SuspiciousRcloneDataExfil
Detects process creation event of executables from suspicious paths	SuspiciousPathProcessCreation
A process tree pattern that matches AsyncRat was detected	AsyncRatProcessChain
Etw bypassed along with hook removal	NtdllHookRemovalEtwBypass
Etw bypassed along with hook removal	KernelDllHookRemovalEtwBypass
Detected Latrodectus process chain	LatrodectusAttackChain
Detects the manipulation of datetime servers in the registry using PowerShell	ManipulateDatetimeServersPowershellProcessCreate
Detects attempts to enable RDP through registry settings using PSEXEC	EnableRDPViaBatchUnderPsExec
Detects LSASS dump by using SilentProcessExit registry	SilentProcessExitLsassDump
Detects execution of unsigned binary through Microsoft SQL Server (SQL injection exploitation)	SqlServerUnsignedBinaryExecution
Detects execution of a possible trojan that was downloaded from a Torrent Client	TorrentClientSuspectedTrojan
Detects attempts to add a domain admin using PowerShell	AddDomainAdminViaNetUnderPsExec
Detects possible NetSupportRat attack chain	PossibleNetSupportRatProcessChain
Explorer loaded suspicious shell extension from installer	ExplorerLoadShellExtensionFromInstaller
Detects net.exe use to attempt to add a domain admin with a low integrity process	AddDomainAdminViaNetLowIntegrity

Barracuda Managed XDR™

Description	Behavioral Indicator
Detects attempts to add a domain admin by a low or medium integrity process	AddDomainAdminViaNetUnderPowershell
Detects forbidden execution by dialer.exe	DialerSpawn
Detects forbidden driver load by dialer.exe	DialerDriverLoad
Detects Krueger Evasion Tool	SuspiciousWDACPolicy
Detects Krueger Evasion Tool	RemoteEDRTamperingAbusingNewWDAC
An interpreter enabled BitLocker Drive Encryption (BDE), indicating a possible ransomware attempt	ModifyEnableBDEWithNoTPMFromInterpreter
A Forbidden spawn enabled BitLocker Drive Encryption (BDE), indicating a possible ransomware attempt	ModifyEnableBDEWithNoTPMFromForbiddenSpawn
Regedit enabled BitLocker Drive Encryption (BDE), indicating a possible ransomware attempt	ModifyEnableBDEWithNoTPMFromRegedit
A reg command enabled BitLocker Drive Encryption (BDE), indicating a possible ransomware attempt	ModifyEnableBDEWithNoTPMFromReg
An interpreter added BitLocker authentication on startup, indicating a possible ransomware attempt	ModifyUseAdvancedStartupFromInterpreter
Detects LanmanServer impersonation	Detects LanmanServer impersonation
Detects when an unauthorized write-to-system partition is performed	AntiVirusEvasionModifyEfiSystemPartitionFileExtended
Detected reflective loading from a process with DotNet loaded after startup	ReflectiveLoadingFromDynamicDotNet
An interpreter enabled BitLocker Drive Encryption (BDE), indicating a possible ransomware attempt	ModifyEnableBDEWithNoTPMFromInterpreter
A Forbidden spawn enabled BitLocker Drive Encryption (BDE), indicating a possible ransomware attempt	ModifyEnableBDEWithNoTPMFromForbiddenSpawn
Detects the combination of bypassing Event Tracing for Windows (ETW) and Antimalware Scan Interface (AMSI) using reflection in PowerShell	MultipleEDRReflectionEvasion
Detects commands from a remote service	RemoteCommandService
Detects when a file is renamed to an alternate data stream	RenamedFileToAds
Detected an attempt to download and execute a file with a scheduled task	ScheduledTaskFromDownload
Detects certutil downloading and subsequent service creation	ServiceCreatedFromCertUtilDownload

Barracuda Managed XDR™

Description	Behavioral Indicator
Detects when a process registered a custom extension to a forbidden process with the command line	SuspiciousCustomExtensionWithCli
Detects PreviousMode exploitation by a process	PreviousModeExploitation
A reg command added BitLocker authentication on startup, indicating a possible ransomware attempt	ModifyUseAdvancedStartupFromReg
Detected misuse of IE4Uinit.exe to execute malicious code	IE4UinitMaliciousExecution
A Suspicious Lumma Stealer Identified	SuspiciousLummaStealerCommandChain
Detected DLLs with cloud file reparse points loaded into PPL processes	CloudReparsePointDllLoadInPplProcess
Detects when a file is renamed to an alternate data stream and deleted	DeletedFileRenamedToAds
Detects process calling of a kernel live-dump from the SentinelOne Agent	KernelLiveDumpViaSentinel
A forbidden spawn added BitLocker authentication on startup, indicating a possible ransomware attempt	ModifyUseAdvancedStartupFromForbiddenSpawn

New AI indicators for analysis and threat hunting:

Description	Behavioral Indicator
Detects DLL hijacking followed by an injection attempt to a system-signed process	DllHijackedProcessInjectedIntoSystemProcess
Detects image load using encoded powershell command	MaliciousImageLoadUsingEncodedPowershell
Detects that an application was hijacked by a suspicious DLL	DLLHijackingD
Detects that an application was hijacked by a suspicious DLL	DLLHijackingE
Detects the access to suspicious cloudflare domain	CloudflareExfiltration
Detection execution of process with multiple extension	PossibleExtensionMasqueradingUnsigned
Detection execution of process with multiple extension	PossibleExtensionMasqueradingSigned

Barracuda
Managed XDR™

Description	Behavioral Indicator
Detects execution of malicious remote Chromium debugger	ChromiumRemoteDebugging
Detects creation and modification of an ADS on a subdirectory in system root	SystemRootSubDirectoryADS
Detects use of the Athena Agent used in Mythic C2	Mythic_C2_Athena_Agent_49213f
Detects use of the Hannibal Agent used in Mythic C2	Mythic_C2_Hannibal_Agent_03262e
Detects reflectively loaded DLL	ReflectiveLoadedDll_ErasedMZ ReflectiveLoadedDll_ErasedMZandPE
Detects mshta process creation by a script downloaded from the internet	MshtaCreatedByWscriptWithZoneIdentifier
Detects interpreter created by an mshta process with a URL in command line	InterpreterFromMshtaUrl
Detects obfuscated interpreter created by an mshta process with a URL in command line	ObfuscatedInterpreterFromMshtaUrl
Detects interpreter created by an mshta process with a downloaded file	InterpreterFromMshtaDownloadedFile
Detects obfuscated interpreter created by an mshta process with a downloaded file	ObfuscatedInterpreterFromMshtaDownloadedFile
Remote process dumped local machine hive locally	DumpLocalMachineHiveRemote
Detects suspicious code Integrity policy creation	SuspiciousCIPolicy
Detects Krueger Evasion Tool	RemoteEDRTamperingAbusingExistingWDAC
Suspicious Powershell Commands Abuse	SuspiciousPowershellInputRedirection
Detect signed DLL Hijacking attempts against SentinelOne binaries	SignedDllHijackingSentinelOneBinary
Detect DLL Hijacking attempts against SentinelOne binaries	DllHijackingSentinelOneBinary
Detect access to telegram api	AccessToTelegramApi
Detects infostealer that exflitrate data with telegram api	InfoStealerTelegramExfiltration

Barracuda
Managed XDR™

Description	Behavioral Indicator
Detects regsvr or rundll execution with a suspicious target file extension	CodeRunnerSuspiciousExtension
Detects creation of a process from an ADS whose host executable was not downloaded	CreateProcessFromAdsNoZoneIdAc
Detects creation and modification of an ADS on a file in the system root directory	SystemRootADS
Detects creation and modification of an ADS on a subdirectory in system root	SystemRootSubDirectoryADS
Detect usage of netsh or reg to enable RDP	EnableRDP
Detects interpreter created by an mshta process with a URL in command line	InterpreterFromMshtaUrl
Detects obfuscated interpreter created by an mshta process with a URL in command line	ObfuscatedInterpreterFromMshtaUrl
Detects interpreter created by an mshta process with a downloaded file	InterpreterFromMshtaDownloadedFile
Detects obfuscated interpreter created by an mshta process with a downloaded file	ObfuscatedInterpreterFromMshtaDownloadedFile
Detects remote System harvesting from VSS	VssSystemHarvestingRemote
Detects System harvesting from VSS by a read handler	VssSystemHarvestingFromRead
Detects System harvesting from VSS	VssSystemHarvesting
Detects remote Sam harvesting from VSS	VssSamHarvestingRemote
Detects Security harvesting from VSS by a read handler	VssSecurityHarvestingFromRead
Detects Security harvesting from VSS	VssSamHarvestingRemote
Improved scheduled task detection	ScheduledTaskNoInteractionWithZoneTaint
Detects when a process tries to disable the System Restore scheduled task	SystemRestoreScheduledTaskTampering
Detects the execution of older version of SharpUp	SharpUpExecuted
Detects interpreter processes and script runs under WinRM	ScriptExecutedUnderWinRM

Barracuda
Managed XDR™

Description	Behavioral Indicator
Detects interpreter processes and script runs under WinRS	ScriptExecutedUnderWinRS
Detects CMD execution under WinRM	CmdExecutionUnderWinRM
Detects CMD execution under WinRS	CmdExecutionUnderWinRS
Detects indirect command execution under WinRM	IndirectExecutionUnderWinRM
Detects indirect command execution under WinRS	IndirectExecutionUnderWinRS
Detects interpreter chaining under WinRM	InterpreterChainingUnderWinRM
Detects lolbin chaining under WinRM	LolbinChainingUnderWinRM
Detects lolbin chaining under WinRS	LolbinChainingUnderWinRS
Detects when a system call is executed from outside a designated syscall function in ntdll, due to code injected by a remote process	KernelCallbackDirectSyscallInjectedCodeCave
Detects an abuse attempt of an accessibility feature binary	AccessibilityFeatureAbuse
Detects Sam harvesting from VSS	VssSamHarvestingExtended
Detects Sam harvesting from VSS by a read handler	VssSamHarvestingFromReadExtended
Detects when a process deletes the SD of a scheduled task	ScheduledTaskSecurityDescriptorDeleted
Detects when a user is created with a non-standard name	HiddenUserName
Detects when a process changes its name in the PEB	PEBProcessNameChanged
Detects process downloading and subsequently executing a .NET assembly in memory	DotNetStagerDownloadedAssembly
Detected a process attempting to interfere with its own EDR DLL	EdrDllLocalTamperingAttempt
Detected a process attempting to interfere with the EDR DLL of another process	EdrDllRemoteTamperingAttempt

Barracuda Managed XDR™

Description	Behavioral Indicator
Detects when a process modifies the security descriptor of a service	ServiceSecurityDescriptorModified
Detected a malicious dotnet assembly loaded from a buffer	MaliciousDotnetAssemblyLoadedFromBuffer
Detects the enumeration phase using AI.	SuspiciousDiscoveryByAI
Detects the enumeration phase using AI.	MaliciousDiscoveryByAI
Detects usage of AuditCode WMI class to execute malicious code	WmiAuditCodeClassUsage
Detects usage of suspicious WMI classes using powershell	SuspiciousWMIQueriesInPowershell
Detects suspicious scheduled task registration from PowerShell	PowerShellScheduledTaskWithoutInteraction
Detects processes that copies chromium password or cookie databases using the CopyFile API	ChromiumDatabaseCopy
Detects processes that copies the chrome password or cookie database using the CopyFile API	ChromeDatabaseCopy
Found an IStorage operation. This privilege elevation technique is used by many NTLM relay tools (Remote Potato, Bad Potato, Juicy Potato, etc...)	UnusualIStorageOperation
Alerts when a signed process with low integrity successfully creates a process with system privileges. It might indicate a LPE exploit	SignedExploitPrivesc
Process deletes its group root signed main content	HidingTracksSigned
If the file was moved to a path (listed in the agent) that requires elevation - make sure that the action was performed via IFileOperation or via wusa, as in common UAC bypass methods	UACBypassSigned
Triggers when a registry value is created (or renamed) with a name which contains a null ('\\0') char by verified process	RegistryHiddenValue
Detects signed processes that write to lsass remotely	SensitiveMemoryAccessRemotely

Barracuda
Managed XDR™

Description	Behavioral Indicator
Detects puppet svchost.exe	UnsualProcessCreation
Detects addition/modification to the BitLocker recovery message	BitLockerRecoveryMessageModify
Detects an abuse attempt of an accessibility feature binary	ReflectiveLoadedDll_ErasedMZ
Detects remote access tool dropped and executed by a LOLbin	ReflectiveLoadedDll_ErasedMZandPE
Detects remote access tool dropped and executed by a LOLbin	LolbinDroppedAndExecutedKnownRAT
Detects remote access tool dropped and executed by a LOLbin	LolbinDroppedAndExecutedUnsignedKnownRAT
Detects remote access tool dropped and executed by an unexpected process	SuspiciousProcessDroppedAndExecutedKnownRAT
Detects remote access tool dropped and executed by an unexpected process	SuspiciousProcessDroppedAndExecutedUnsignedKnownRAT
Detects remote access tool dropped and executed by an unexpected process	SuspiciousKnownRATExecution
Detects remote access tool dropped and executed by an unexpected process	SuspiciousUnsignedKnownRATExecution
Detects process performing module stomping in its own address space	ModuleStompingLocal
Detects process performing module stomping in another process's address space	ModuleStompingRemote
Detects ADFS service hijacking	AdfsServiceHijacking
Lsass loaded an extension library	LsassSspLibraryLoad
Detects writable process creation	WritableProcessCreation
Detects tampering of AMSI related registry	PossibleRegistryAmsiBypass
Printer driver added, might indicate printNightmare exploit	PrinterDriverAdded
A process registered a custom extension with command line	RegistryCustomExtension
Detects when a task is created and is set to run known application	KnownTaskCreated

Barracuda Managed XDR™

Description	Behavioral Indicator
Detects statically linked DLL Hijacking - loading unsigned library which exists as signed in System directory	PossibleStaticDllHijack
Detects initialization of security context	SecurityContextInitialization
Detects when a process opens sitelist.xml, a file belonging to McAfee that might contain passwords	PossibleMcAfeeInfoStealing
Detects possible credentials harvesting from VSS	PossibleVssCredsHarvesting
Detects file harvesting via direct volume access	DirectVolumeFileHarvestingKnown
Detects Dll Hijacking by signed and known library	PossibleDllHijackingByKnownLibrary
Detects non powershell signed processes that load powershell module System.Management.Automation.dll or System.Management.Automation.ni.dll	PowershellWithoutPowershellExeSigned
Detects loading of signed AMSI DLL to a process	SignedAmsiDllHijack
Detects infostealing from two or more of the following applications: Chrome, Firefox, Chromium Edge, Windows vault, FileZilla, Opera by signed and known process	MultipleInfostealersByKnownProcess
Detects Kerberos related attacks	KerberosAbuse
Application overwrote an existing com object with a new signed one. Triggered when a value named \CodeBase\ or with an empty name, under [\CLSID*\\\\InprocServer32\, \Classes*\\\\CLSID*\\\\InprocServer32\] is set or deleted.	RegistryComPersistenceSignedObject

Contact the SOC if you have any questions.

Thank you.