Cylance Endpoint Security

Release Notes

Contents

Cylance Endpoint Security service updates

Product	Latest release
Management console and platform services	April 2024
CylancePROTECT Desktop	January 2024
CylancePROTECT Mobile	March 2024
CylanceOPTICS	January 2024
CylanceGATEWAY	April 2024
CylanceAVERT	April 2023

Management console and platform services

This section contains information about updates to the management console and platform services that impact more than one Cylance Endpoint Security service or the general experience of the console. Console changes that impact specific Cylance Endpoint Security services are described in the respective sections of this guide.

What's new in the management console

Feature	Description	Date added
Alerts view enhancement	The Alerts view now supports CylancePROTECT Desktop script control alerts, including the ability to add a file associated with a script control alert to the global safe list. For more information, see Managing alerts across Cylance Endpoint Security services in the Cylance Endpoint Security Administration content.	April 2024
Alerts view enhancements	• After you filter alert groups by the desired criteria, you can now select and bulk delete all of the alert groups in the filter results, or select alert groups. • You can now export alert groups or the alerts within a group in JSON format. For more information, see Managing alerts across Cylance Endpoint Security services in the Cylance Endpoint Security Administration content.	March 2024
Console sign in enhancement	By default, new tenants now require administrators to enter a one-time password, in addition to the Cylance console password, each time that they try to access the console. Existing customers can update the authentication policy to add the One-Time Password requirement. New tenants can remove the One-Time Password requirement after an administrator sign-in to the console for the first time. For more information, see Enhanced authentication sign in.	March 2024
User Policy enhancements	The following enhancements have been made to the "Add User or Group" setting (Policies > User Policy) in the management console: • You can now search for users and user groups under separate tabs. • The search results are displayed in alphabetical order based on a user's or user group's name. • By default, a maximum of 50 search results are returned for users and groups, respectively. Administrators must refine their search criteria when more than 50 search results are returned.	February 2024

Feature	Description	Date added
Support for IDP-initiated Single Sign On	Administrators can now configure their environment so that users can access the Cylance console directly from their Identity provider (IDP). If your authenticator was created before December 2023, you can update their environment to enable IDP-initiated Single Sign On to the Cylance console. For more information, see Enhanced authentication sign in.	December 2023
Alerts view enhancements	• When you view the details of an alert group that contains CylancePROTECT Desktop threat alerts, you now have the option to add a file to or remove a file from the global safe list or global quarantine list. • When viewing alert groups and details for individual alerts, key indicators (script, process, file, and so on) are now represented by icons. You can click a key indicator icon to access different options where applicable, including view (to see full text string values), copy, and filter. • When you view the details for an alert group or an individual alert in a group, you can now see a visual representation of the relationship between key indicators (files, users, executables, processes, and so on). • You can now add an Okta connector to the Cylance console to surface Okta authorization and access alerts in the Alerts View. • You can now add a Mimecast connector to the Cylance console to surface Mimecast risk attachment alerts in the Alerts View. For more information, see Managing alerts across Cylance Endpoint Security services in the Cylance Endpoint Security Administration content.	November 2023
New JRE requirement for the BlackBerry Connectivity Node	The latest version of the BlackBerry Connectivity Node (2.14) requires JRE 17. To download the latest version of the BlackBerry Connectivity Node, click here. For more information, see Set an environment variable for the Java location in the Cylance Endpoint Security Setup content.	November 2023
Alerts view enhancements	• You can now export detailed information for alert groups and the individual alerts within a group to a CSV file. • More options have been added for text-based filtering to allow you to efficiently build and modify alert filters. For more information, see Managing alerts across Cylance Endpoint Security services in the Cylance Endpoint Security Administration content.	October 2023

BlackBerry Connectivity Node version

BlackBerry Connectivity Node version 2.14.0. To download the latest version of the BlackBerry Connectivity Node, click here.

Management console and platform services fixed issues

Management console

When there were too many device requests to update the CylancePROTECT Desktop agent and updates were throttled by the console, after four attempts by the device, the device was temporarily blocked from receiving the agent update. (EPCL-2100)
In the multi-tenant console, when you tried to import an exclusions .csv file for the External Device Control device policy, the "Sorry, something went wrong; please try again later" error message appeared. (EPCL-1632)
When requesting a threat data report, the request was not automatically retried before it was finally determined to be unsuccessful. (EPCL-1718)
Some CylanceOPTICS rule categories were missing in the SAE1, EUC1, APNE1, and APSE2 regions and needed to be manually imported. (EPCL-471)
When a device was automatically assigned another policy through a new zone rule, the Cylance audit log was missing information about which policy was applied to the device. (EPCL-1889)
When you assigned a zone with devices to the “Test” or “Pilot” zone-based update rules, if the zone had devices with an update available, the target agent version for the device was not specified in the console properly. (EPCL-3)
On the Protection > Threats screen of the Cylanceconsole, you could not add specific threats to the safe or quarantine list. (EPPCL-2588)

Entra ID Synchronization

You could not authenticate users synchronized from Entra ID if the user's email address and UPN did not match. (EID-16967)

Authentication

If the maximum session age specified in a client was less than the default setting used by Okta, users that completed Okta authentication were not prompted to reauthenticate until the session age set in Okta was reached. This was due to a known Okta issue. (EID-17965)

BlackBerry Connectivity Node

BlackBerry Router and proxy settings displayed in the BlackBerry Connectivity Node were not applicable to CylanceGATEWAY. (UES-6396)

Management console and platform services known issues

Management console

In Google Chrome version 105.0.5195.102 and later, the "Block third-party cookies" option is enabled by default for incognito mode. If you try to log in to the management console while this option is enabled, you may receive a "Sign-in failed" error. (UES-9770)

Workaround: Change your Chrome privacy and security settings to allow all cookies, or in the browser settings add [*.]cylance.com as a site that can always use cookies.

Dashboards

The management console user details (Assets > Users) does not display the TLS version in the CylanceGATEWAY event details screen when the CylanceGATEWAY agent is installed and activated. For more information, visit support.blackberry.com to read article 99220. (BIG-6300)

The management console unprotected devices screen (Assets > Unprotected devices) occasionally may display incorrect device OS and OS versions. For example,

- On Mac devices, supported OS and OS versions may display as unknown and unsupported, respectively. (UES-9904)
- On Windows devices, unsupported OS versions (for example, Windows Server 2008 and Windows 8) may display as supported. (UES-9903)

For information about the operating systems that each of BlackBerry Protect Desktop agents supports, see the Cylance Endpoint Security compatibility matrix.

The management console unprotected devices screen (Assets > Unprotected devices) incorrectly displays devices running Windows 10 Enterprise Insider Preview as Linux (UES-9897)

The management console unprotected devices screen (Assets > Unprotected devices) does not display the device OS and OS version and results in 'insufficient information' to be displayed for the devices. (UES-9574)

Workaround: Configure the schema to allow the required attributes to synchronize from the domain controller to the Global Catalog. For instructions, see Configure your environment to view the device OS and OS version of managed unprotected devices in the administration content.

BlackBerry Connectivity Node

The BlackBerry Connectivity Node is not compatible with OpenJDK292b10 or ZuluJDK292b10. (UES-3667)

A Java bug for this issue has been logged at https://bugs.java.com/bugdatabase/view_bug.do?bug_id=JDK-8266279.

CylancePROTECT Desktop release notes

The following tables provide information about the new features of CylancePROTECT Desktop in the management console. For the agents, information is available in their separate sections:

- Windows agent
- Linux agent
- macOS agent

What's new in the management console for CylancePROTECT Desktop (January 2024)

Feature	Description
Software inventory (Windows only)	This feature allows administrators to identify applications that may be a source of vulnerabilities, prioritize actions against vulnerabilities, and address them accordingly. Administrators can view all applications installed on devices that are registered with the tenant and view a list of applications that are installed on individual devices. • Administrators can enable this feature for devices through the device policy in the **Agent Settings** tab. • Devices must be running CylancePROTECT Desktop agent version 3.2 or later. • To view a list of all applications installed on devices, navigate to **Assets > Installed Applications** in the console. • To view a list of applications on an individual device, navigate to **Assets > Devices > Threats & Activities > Installed Applications** in the console.
Enhanced script control using script scoring (Windows only)	The CylancePROTECT Desktop agent now supports enhanced script control using script scoring. Scripts that have an unsafe or abnormal threat score can be intelligently blocked from executing and alerted to the management console. • Devices must be running CylancePROTECT Desktop agent version 3.2 or later. Devices running unsupported agents will default to block scripts. • Administrators can configure the Active Script or PowerShell Script setting from the Script Control tab in the device policy to block scripts that CylancePROTECT considers to be unsafe or abnormal. For more information, see the Cylance Endpoint Security Setup content.
Alert mode for the use of PowerShell Console (Script control for Windows only)	The CylancePROTECT Desktop agent now supports Alert mode for the use of PowerShell Console in interactive mode, so that detected events are reported to the management console while still allowing them to run. • Devices must be running CylancePROTECT Desktop agent version 3.2 or later. Devices running unsupported agents will default to block the use of PowerShell console. • Administrators can control the setting from the Script Control tab in the device policy using the PowerShell Console drop-down menu.

What's new in the management console for CylancePROTECT Desktop (October 2023)

Feature	Description
Background threat detection on-demand scan	Administrators can now initiate a background threat detection scan on demand from the management console. • Devices must be running CylancePROTECT Desktop agent version 3.2 or later. • The command can be sent from the Device Details screen for an individual device, or for multiple devices at once from the Devices screen. Note that if background threat detection scans are running on several VM devices that are from the same VM host at the same time, device performance will be impacted due to resource sharing.

What's new in the management console for CylancePROTECT Desktop (May 2023)

Feature	Description
DLL exclusions for memory protection (Windows only)	In the device policy, you can now add memory protection exclusions for third-party application DLLs. For example, if you are running third-party security products in addition to CylancePROTECT, you can add an exclusion for the appropriate .dll files so that CylancePROTECT ignores specific violations for those products. This feature supports the Malicious Payload and System DLL Overwrite violation types only. The following rules apply when you specify a DLL exclusion: • You must select the **Treat as DLL exclusion** option in the device policy. • The device must be running CylancePROTECT Desktop agent version 3.1.1001 or later on a Windows device. • The exclusion file path that you specify must be the full, direct path to the .dll file. Wildcards are not allowed. • The .dll file must be signed using a certificate that is trusted on the device where CylancePROTECT Desktop is installed. Otherwise, it will not be excluded.

What's new in the CylancePROTECT Desktop agent for Windows

What's new in Windows agent version 3.2.1001

Bug fixes only. See fixed issues.

What's new in Windows agent version 3.2.1000

Feature	Description
Software inventory	The CylancePROTECT Desktop agent now reports a list of applications that are installed on devices to the management console. This feature allows administrators to identify applications that may be a source of vulnerabilities, prioritize actions against vulnerabilities, and address them accordingly. Administrators can view all applications installed on devices that are registered with the tenant and view a list of applications that are installed on individual devices. This feature can be enabled for the agent from the device policy in the Agent Settings menu. See Agent settings.
Background threat detection on-demand scan	Administrators can now initiate a background threat detection scan on demand from the management console. The command can be sent from the Device Details screen for an individual device, or for multiple devices at once from the Devices screen. The date of the last scan for each device is logged in the management console. See Manage CylancePROTECT Desktop and CylanceOPTICS devices. Note that if background threat detection scans are running on several VM devices that are from the same VM host at the same time, device performance will be impacted due to resource sharing.
Enhanced script control using script scoring	The CylancePROTECT Desktop agent now supports enhanced script control using script scoring. Scripts that have an unsafe or abnormal threat score can be intelligently blocked from executing and alerted to the management console. Administrators can configure the script control settings in the device policy to block scripts that CylancePROTECT considers to be unsafe or abnormal. See Script control.
Alert mode for PowerShell Console scripts (Script control)	The CylancePROTECT Desktop agent now supports Alert mode for PowerShell Console scripts, so that detected events are reported to the management console while still allowing them to run. Administrators can control the setting from the Script Control tab in the device policy using the PowerShell Console drop-down menu. See Script control.
Windows OS support	Due to legacy and technical limitations, the CylancePROTECT Desktop agent version 3.2 does not support the following Windows OSs: • Windows 7 • Windows Server 2012 (Standard, Data Center, Essentials, Server Core, Embedded & Foundation) These versions of Windows are supported by CylancePROTECT Desktop version 3.1.x.

What's new in Windows agent version 3.1.1003

Bug fix only. See fixed issues.

What's new in Windows agent version 3.1.1001

Feature	Description
Script control improvements	The CylancePROTECT Desktop agent now reports parent and interpreter processes to the Cylance console when a potentially malicious script is executed. Administrators can add exclusions for either a parent process or interpreter process of a script to allow the script to run on a device.
DLL exclusions for memory protection	The CylancePROTECT Desktop agent for Windows now supports the ability to add exclusions for third-party application DLLs. For example, if you are running third-party security products in addition to CylancePROTECT, you can add an exclusion for the appropriate .dll files so that CylancePROTECT ignores specific violations for those products. This feature supports the Malicious Payload and System DLL Overwrite violation types only. The following rules apply when you specify a DLL exclusion: • You must select the **Treat as DLL exclusion** option in the device policy. • The device must be running CylancePROTECT Desktop agent version 3.1.1001 or later on a Windows device. • The file path that you specify must be the full, direct path to the .dll file. Wildcards are not allowed. • The .dll file must be signed using a certificate that is trusted on the device where CylancePROTECT Desktop is installed. Otherwise, it will not be excluded.
Improvements to memory protection sensor for malicious payloads	The memory protection sensor for the malicious payload violation type has been improved to help improve accuracy of violation reporting and reduce unnecessary alerts.

What's new in Windows agent version 3.1.1000

Feature	Description
Execution protection for XLM/XL4 Excel Macros (Preview)	The CylancePROTECT Desktop agent now works with Microsoft's anti-malware scan interface (AMSI) so that when a potentially dangerous XLM macro is executed, threat information is reported to the management console, and the agent responds to the interface according to the device policy rules for script control events. For example, the agent responds whether to allow the macro to run or block it from running. This feature is enabled from the Script Control > XLM Macros settings in the device policy. This feature requires the following: • Microsoft Windows 10 or later • CylancePROTECT Desktop agent version 3.1 • VBA macros must be disabled in the Excel **File > Trust Center > Excel Trust Center > Macro Settings** menu. **Note:** This feature is currently available in Preview mode where it might behave unexpectedly.
Support for Antimalware Protected Process Light (AM-PPL)	The CylancePROTECT Desktop agent now runs as a trusted service using Antimalware Protected Process Light (AM-PPL) technology from Microsoft, which protects the agent's security processes from malicious actions. For example, it helps protect the agent from being terminated. This feature requires the endpoint to be running Windows 10 1709 or later or Windows Server 2019 or later.
Custom interval for background threat detection scanning	Administrators can now set a custom interval to run background threat detection scanning from the device policy. The scan interval can be set between 1 and 90 days. The default scan interval is 10 days. Note that increasing the frequency of the scans might impact the device performance. The scan may also be manually started from the command line.
Manually start background threat detection scanning	On Windows devices, you can now manually start background threat detection scanning from the command line using the `backgroundscan` command option. For example, you can run the following command: `C:\Program Files\Cylance\Desktop\CylanceSvc.exe /backgroundscan`
Windows OS support	• Added support for Windows 365 (Business, Enterprise) • Added support for Windows 10 (22H2) • Removed support for Windows 10 (2004)

What's new in Windows agent version 3.0.1005

Feature	Description
LSASS Read violations reporting	LSASS Read violations that are blocked are now reported to the management console.

Note: Due to compatibility issues, tenants that have CylanceOPTICS 3.2 for Windows available will not have CylancePROTECT Desktop agent version 3.0.1005 for Windows provisioned to them. The compatibility issues will be resolved in an upcoming release. All other versions of CylanceOPTICS support CylancePROTECT Desktop agent version 3.0.1005 for Windows.

What's new in Windows agent version 3.0.1000

Feature	Description
Support for Windows 11	The CylancePROTECT Desktop agent for Windows now supports Windows 11 devices.
LSASS Read violations detection	Detection of LSASS Read violations has been improved in the Windows agent 3.0.1000.
Exclusions for macro files	For Windows devices running agent 3.0.1000, administrators can now add exclusions in the Memory Protection device policy for macro files that cause Script Control events.
Read-only access to USB devices	For Windows devices running agent 3.0.1000, administrators can now allow read-only access to external USB devices on Windows devices.
Detection disabled for embedded VBScripts	Detection of embedded VBScript script control violations is disabled in Windows agent 3.0.1000.

What's new in Windows agent version 2.1.1584

Feature	Description
Added support for Windows	The CylancePROTECT Desktop 2.1.1584 agent for Windows is supported on devices running Windows 10 21H1 (May 2021), Windows 10 21H2 (November 2021), Windows 11, and Windows Server 2022.
Memory protection enhancements	• Memory Protection now uses a new code base and methodology that generates more events. • The Dangerous VBA Macro event (RunMacroScript) is now a memory protection event, not a script control event. This event prevents dangerous implementations within a macro. This event is not related to running scripts.

What's new in Windows agent version 2.1.1568

Bug fixes only

Note: The CylancePROTECT Desktop 2.1.1568 agent for Windows is the last release that supports endpoints running the Windows XP, Windows Server 2003, and Windows Server 2008 (non-R2) operating systems. The Cylance SHA1 certificate that the agent requires to support these endpoints is due to expire in November 2023. After November 2023, any endpoints that are running this version of the agent may not behave as expected. For endpoints that are running a later version of Windows, you must install a later version of the CylancePROTECT Desktop agent. For more information about CylancePROTECT Desktop support for legacy operating systems, visit support.blackberry.com and read KB 66653.

Fixed issues in the Windows agent

Fixed in Windows agent version 3.2.1001

An issue that prevented the offline ML model from working properly on Windows devices running CylancePROTECT Desktop version 3.2.1000 was fixed. (EPP-4880)
Some files that could not be scored in the Cylance cloud or locally received invalid scores which caused unnecessary log entries. (EPP-4662)
Some files that could not be scored in the Cylance cloud or locally were repeatedly analyzed which caused unnecessary log entries. (EPP-4661)
After a USB device such as a document scanner was unplugged and you plugged in another one, and the device control policy was turned on, a system bug check (SYSTEM_THREAD_EXCEPTION_NOT_HANDLED) error occurred and the device was forced to reboot. (EUS-1685)
If a USB device was connected at device startup, sometimes the device control policy blocked it even though there is a valid exclusion set in the device policy. (EUS-1424)
Some USB4 docking stations did not work properly after a device restart on a device that had device control policy enabled. (EUS-1400)
If you plugged in a UGREEN USB-C hub on a device that was running the CylancePROTECT Desktop agent with a device control policy, a blue screen error occurred. (EUS-934)

Fixed in Windows agent version 3.2.1000

When Auto Quarantine was enabled, the OS might hang temporarily while CylancePROTECT Desktop took some time to process unknown files. (CHP-8912)
When you try to install Autodesk on a device with the Block PowerShell Console Usage device policy rule enabled, you were blocked. (CHP-8861)
When attempting to upgrade the CylancePROTECT Desktop agent from version 3.x to 3.2, the CylanceSvc could not restart and the upgrade was not successful. (EPP-4424)
Compressed archives that contained executables were not scored properly. The "Input stream of wrong type: stream must be readable and seekable but not writeable" error message appeared in the log file. (EPP-4083)

When the Cylancesvc service was restarted, the timestamp for the last background threat detection scan was updated even though a scan did not take place after the service restarted. (EPP-3958)
If the device has a copy of one of the CylancePROTECT Desktop agent assemblies or .dll files referenced in the .NET Global Assembly Cache (for example, System.Data.SQLite.dll), the CylancePROTECT Desktop agent could not start properly. (EPP-3767)
Each time an executable that was in the exclusion list was run on a device, there were multiple redundant 'UNKNOWN_FILE' log entries associated with it. If the executable was used frequently, the log file size can grew quickly. (EPP-2828)
When you use the online updater to upgrade the CylancePROTECT Desktop agent, if its installation was successful but the upgrade of a non-CylancePROTECT Desktop agent (such as CylanceOPTICS) was not successful, the CylancePROTECT Desktop agent was rolled back unnecessarily. If the upgrade to CylancePROTECT Desktop agent 3.2 is successful, it does not roll back even if upgrades to other agents were not successful. (EPP-1897)
When a file in the global quarantine list was detected and blocked, the block action was not reported to the management console if the file was deleted before the agent processed the event. (EPP-1709)
After unplugging a USB device such as a document scanner and then plugging in another one, and the device control policy is turned on, a bug check error occurs and the device is forced to reboot. (EUS-1655)
When both PowerShell Console and PowerShell Script policies are set to Block, some scripts were blocked from running even though they should have been allowed according to script control exclusions. (EUS-1212, EUS-1123)
After plugging in a USB device such as a printer through a USB hub, and the device control policy is turned on, a bug check error occurs and the device is forced to reboot. (EUS-563)

Fixed in Windows agent version 3.1.1003

If the device has a copy of one of the CylancePROTECT Desktop agent assemblies or .dll files referenced in the .NET Global Assembly Cache (for example, System.Data.SQLite.dll), the CylancePROTECT Desktop agent could not start properly. (EPP-4507, EPP-3767)

Fixed in Windows agent version 3.1.1001

When a device could not connect to the Cylance management console, the log line that was associated with the event was only available when verbose logging was enabled. (EPP-3311)
If you installed a version of CylancePROTECT Desktop using a unified installer (version 2.4.x), you were prevented from upgrading the CylancePROTECT Desktop agent individually. You can now upgrade to CylancePROTECT Desktop agent 3.1.1001.17 using the online updater. (EPP-3300) For more information, visit support.blackberry.com/community to read KB 102884.
When a device connection timed out, the log line that was associated with the event was only available when verbose logging was enabled. (EPP-3294)

Devices that are on networks with higher latency could not connect to Cylance Cloud services. (EPP-3292)
When you opened Microsoft Excel documents through an Outlook attachment or OneNote tab, `OfficeClickToRun.exe` was blocked by the memory protection policy. (EPP-1951)
The `taskkill.exe` process intermittently stopped responding while killing a process. (EUS-1274)
In a Citrix VDI environment, high CPU usage by the CylancePROTECT Desktop agent was observed. (EUS-1209)
When a memory protection exclusion for Dangerous VBA macros was added for a .xlsm file, if file name contained Japanese characters, the file was not excluded properly and was blocked from running. (EUS-1090)

Fixed in Windows agent version 3.1.1000

When Smart App Control was enabled on Windows 11 devices, the installation of the CylancePROTECT Desktop agent 3.1 was not successful if you used the .exe installer. (EPP-3194)
When a memory protection violation occurred, there was a delay before the system reported the event to the management console. (CHP-8615)
When some applications caused a memory protection violation, the applications stopped responding due to a "Security check failure or stack buffer overrun" error. (EUS-991)
Microsoft Excel stopped responding due to stack overflow errors when attempting to run a macro with VBA hooking functions. (EUS-664)
When VSTO add-ins are configured in Microsoft Excel, it stopped responding when you opened a file that included various macros even though exclusions were properly set. (EUS-637)
When accessing an ASP-based website that uses an embedded VBScript, the website throws a 500 error on the first attempt to access the site. This error appears if the device is assigned a policy with the Active Script script control setting enabled. (EUS-555)
The memory protection exclusion list did not take effect properly when folders were named using uppercase letters of the Zenkaku Hiragana input method. (EUS-937)

Fixed in Windows agent version 3.0.1005

When “Block PowerShell Console Usage” was selected in the script control policy, and a script that used the Write-Error cmdlet was added to the exclusion list (i.e. approved), the script was interrupted when it used the cmdlet. The script can now run as expected without being interrupted by the agent when the cmdlet is used. (EUS-508)
If the CylancePROTECT Desktop agent version 3.0 with memory protection enabled was running on a user’s 64-bit Windows OS, and the user started a 32-bit version of Microsoft Outlook, Outlook closed immediately. (EUS-440)

When a user tried to execute a program file from a network share while the CylancePROTECT Desktop agent version 3.0 was monitoring, Windows might have displayed a blue screen with the following error: "Your PC ran into a problem and needs to restart, Stop code: SYSTEM_SERVICE_EXCEPTION, What failed: CylanceDrv64.sys" (EUS-437)
When memory protection was enabled, redundant information was written to temporary files. The redundant information has been reduced and fewer temporary files are created. (EUS-294)

Fixed in Windows agent version 3.0.1000

The CylancePROTECT service did not start on devices that have installed the Arabic version of Windows. (CHP-8512)
When you opened the Windows agent on a Windows 10 device, some options were disabled when you right-clicked a threat in the Threats tab. In Online Mode, the "Show File Properties" option was disabled. In Disconnected Mode, "Show File Properties", "Quarantine File", and "Waive File" options were disabled. (CHP-8357)
The timestamps of events that the agent reported were slightly offset if the device time zone was set to UTC +0100. (CHP-8351)

Fixed in Windows agent version 2.1.1584

Microsoft SQL Server 2008 R2 stopped responding on startup. (MEM-847)
Fixed an issue with WideOrbit servers and CylancePROTECT Desktop script control. (MEM-846, MEM-844)
Fixed an issue with Microsoft Dynamics and CylancePROTECT Desktop script control. (MEM-845)
An error occurred when launching VisionApp Remote Desktop 2011 with script control enabled. (MEM-830)
Resolved an issue with LSASS Read for memory protection. (MEM-662)
The agent did not properly log an action taken for the Remote APC Scheduled violation. (CHP-8534)

Fixed in Windows agent version 2.1.1568

When a remote procedure call (RPC) message was larger than 64K and the agent allocated memory, the memory allocation size couldn't be modified. (EPP-1504)
An arbitrary message could have been broadcasted to an Advanced Local Procedure Call (ALPC) port. (EPP-1503)
A user with insufficient privileges could have deleted files in the Cylance directory when using a remote procedure call (RPC) and the Chromium Embedded Framework (CEF) was loaded using a third-party app. (EPP-1236)
A system bugcheck may occur when formatting some Unicode strings for logging. (CHP-8610)

Known issues in the Windows agent

* CylancePROTECT Desktop might not successfully block Microsoft Excel files that are infected with Kangatang or Laroux viruses even though the Dangerous VBA Macros policy is turned on. (EUS-1465)
* If a USB device is connected at device startup, sometimes the device control policy blocks it even though there is a valid exclusion set in the device policy. (EUS-1424) **Workaround**: Disconnect and reconnect the USB device.
* The Barco ClickShare app stops responding when memory protection is turned on in the device policy. (EUS-1283) **Workaround**: Add a memory protection exclusion for `clickshare_native.exe`.
On some devices running Windows Server 2012 R2, `rundll32.exe` stops responding after a memory protection violation. (EUS-1267)
The script control policy for XLM macros is not enforced if the Excel Trust Center > Macros Settings is set to "Enable VBA macros". (EUS-1065) **Workaround**: Verify that one of the "Disable VBA macros" is selected.
When the Windows 8.3 short naming format of a process path is used to execute a file (e.g. `C:\PROGRA~1\folder\file.exe`) and the memory protection exclusions are defined using the long naming format for that process (e.g. `C:\Program Files\folder\file.exe`), the exclusions do not apply. (EUS-593) **Workaround**: Ensure that files are executed using the long path format. Note that adding exclusions using the Windows 8.3 short naming format is not supported.
On a device running Windows Server 2012 R2 and CylancePROTECT Desktop agent 2.1.1580 and later, `System32\wbem\WmiPrvSE.exe` is incorrectly reported as a threat. (EUS-179, EPP-3279)
When trying to launch Microsoft Visual Studio 2022, several System DLL Overwrite violations are reported and it is not launching as expected. (EPP-2312) **Workaround**: In the device policy, add an exclusion to ignore "System DLL Overwrite" violations for devenv.exe that is located in the installation folder of Visual Studio 2022. For example, set the exclusion to ignore "System DLL Overwrite" violations at `\Program Files\Microsoft Visual Studio\2022\Professional\Common7\IDE\devenv.exe`. The installation path may differ between editions and locales.
If you assign a device policy with script control set to "Block" but allow PowerShell console usage, scripts run from the PowerShell console are blocked. (CHP-8409)
On the Script tab of the Windows agent, the command line display in the tooltip for a long PowerShell script shows duplicated and overwritten information. (CHP-8349)
The Cylance service may intermittently get stuck in a “StopPending” state when cycling between a stopped and running state. (CHP-7174)
When "System DLL Overwrite" is enabled in the memory protection policy, using AutoCad 2022 (S.51.0.0) and trying to log in to an AutoCad account triggers a memory protection event. (COM-3896) **Workaround**: Add a memory protection exclusion for AutoCad for the System DLL Overwrite violation type.

What's new in the CylancePROTECT Desktop agent for Linux

What's new in the Linux agent version 3.2.1000

Feature	Description
Added support for Linux distributions	Added support for the following Linux distributions: • Amazon Linux 2023 • Amazon Linux 2, kernel 5.10
Background threat detection on-demand scan	Administrators can now initiate a background threat detection scan on demand from the management console. The command can be sent from the Device Details screen for an individual device, or for multiple devices at once from the Devices screen. The date of the last scan for each device is logged in the management console.

Note: When manually downloading and installing the latest Linux driver, select the latest driver version from the Cylance console to ensure support for the latest kernel update. The latest driver (which is 3.2.1100 currently) is frequently updated with cumulative kernel support and is compatible with CylancePROTECT Desktop agent versions 2.1.1590 and later. Consider turning on the Auto-Update Linux Driver option in the update rule for devices running CylancePROTECT Desktop agent 3.1 or later.

What's new in the Linux agent version 3.1.1001

Feature	Description
Added support for Linux distributions	Added support for the following Linux distributions: • Red Hat Enterprise Linux 9 and 9.1 • Oracle 9 and 9.1 • Oracle UEK 9 and 9.1 • Oracle 8.7 • Oracle UEK 8.7 • SUSE (SLES) 15 SP4
Updated Linux driver package	The Linux driver package version 3.1.1101 is now available from the management console and is compatible with agent version 2.1.1590 and later. If you are using the Auto-update Linux Driver feature, the agent drivers will be updated automatically to version 3.1.1101. The Auto-update Linux Driver feature requires CylancePROTECT Desktop agent version 3.1.1000 and the agent driver version 3.1.1000 or later.

What's new in the Linux agent version 3.1.1000

Feature	Description
Added support for Linux distributions	Added support for the following Linux distributions: Ubuntu 22.04 LTS
Custom interval for background threat detection scanning	Administrators can now set a custom interval to run background threat detection scanning from the device policy. The scan interval can be set between 1 and 90 days. The default scan interval is 10 days. Note that increasing the frequency of the scans may impact the device performance. The scan may also be manually started from the command line. The date of the last scan for each device is logged in the management console.
Auto-update Linux Driver	The CylancePROTECT Desktop agent 3.1.1000 for Linux devices can now request an update to the latest supported agent driver when an updated kernel is detected on the system. For example, if the Linux kernel is updated and the current installed agent driver does not support it, the agent can now automatically update the driver as soon as a compatible driver is released. This feature requires CylancePROTECT Desktop agent version 3.1.1000 and the agent driver version 3.1.1000 or later. To enable this feature, select the **Auto-update Linux Driver** option in the zone-based update rule from the **Settings > Update** menu in the management console.

What's new in the Linux driver version 3.1.1100

The CylancePROTECT 3.1.1100 driver package is now available for Linux endpoints, in advance of an upcoming release of the 3.1 agent. It includes the latest drivers to support the latest OS kernels and is compatible with devices running agent version 2.1.1590 or later. When the driver is used together with the upcoming release of the 3.1 agent, administrators can allow the Linux driver to be automatically updated to support the latest OS kernels. Updating to the latest Linux driver makes sure that CylancePROTECT continues to run as expected while you receive important OS kernel updates.

What's new in the Linux agent version 3.0.1005

Bug fixes only.

If you installed the CylancePROTECT 3.0.1101 or 3.0.1100 driver package for Linux endpoints running the 3.0.1001, 3.0.1000, or 2.1.1590 agents, the drivers are not automatically updated to 3.0.1105 (which includes bug fixes) when the 3.0.1005 agent is deployed from the console or upgraded locally. To update the drivers on endpoints that have the 3.0.1101 or 3.0.1100 driver package installed, manually upgrade to the 3.0.1105 driver package that is available in the Cylance Endpoint Security management console.

What's new in the Linux agent version 3.0.1001

Bug fixes only.

If you installed the CylancePROTECT 3.0.1100 driver package for Linux endpoints running the 3.0.1000, or 2.1.1590 agents, the drivers are not automatically updated to 3.0.1101 (which includes bug fixes) when the 3.0.1001 agent is deployed from the console or upgraded locally. To update the drivers on endpoints that have the 3.0.1100 driver package installed, manually upgrade to the 3.0.1101 driver package that is available in the Cylance Endpoint Security management console.

What's new in the Linux agent version 3.0.1000

Feature	Description
Added support for Linux distributions	Added support for the following Linux distributions: • RHEL/CentOS 8.4 • RHEL 8.5 • Oracle 8.4 • SUSE 12 SP5 • SUSE 15 SP2 and SP3 To view the full list of supported Linux kernels and drivers, download the Supported Linux Kernels spreadsheet.

Fixed issues in the Linux agent

Fixed in Linux agent version 3.2.1000

A new Linux driver could not be loaded even though it was available for devices running recent RHEL 8 kernel versions such as 4.18.0-305.97.1, 4.18.0-305.95.1, 4.18.0-305.93.1, and 4.18.0-305.91.1. (EPP-4171)
When attempting to auto-update the 3.1.1100 driver on a Linux device, the driver was not updated properly even though an update was available. (EPP-4118)
When a file in the global quarantine list was detected and blocked, the block action was not reported to the management console if the file was deleted before the agent processed the event. (EPP-1709)
In the syslog, the 'kernel read not supported for file' log line appeared extraneously. (CHP-8920)

Fixed in Linux agent version 3.1.1001

When the PID number of a process was greater than 32768, a violation that was related to that process was not detected. The fix is also available using driver package version 3.1.1101 for devices running agent 2.1.1590 and later. (EPP-3214)

Fixed in Linux agent version 3.1.1000

When you tried to scan a specific directory that had Japanese characters in its name using the command line option, the scan was not successful. (CHP-8700)

Fixed in Linux agent version 3.0.1005

When the CylancePROTECT driver was extracted from the .tar archive, the folder permissions were unexpectedly changed. The permissions are no longer changed and the folder's original permissions are now properly retained. This issue is fixed in the 3.0.1005 and 3.0.1105 Linux drivers. (EPP-2359)
The deployment of CylanceHYBRID on a host computer was not successful if CylancePROTECT was running with the memory protection policy enabled. (CHP-8676)
High memory usage was identified on Linux devices. This issue is fixed in the 3.0.1005 and 3.0.1105 Linux drivers. (CHP-8661)
If SELinux was disabled after the CylancePROTECT drivers were already loaded, a system kernel panic error occurred. This issue is fixed in the 3.0.1005 and 3.0.1105 Linux drivers.(CHP-8651)

Fixed in Linux agent version 3.0.1001

There was excessive logging of `CefRPCServerHelper:listenForRequests: Error receiving message from queue using conn=## errno=110 (Connection timed out)` in the system logs. For more information visit support.blackberry.com and read KB 93972. (EPP-2239)
When trying to update or uninstall the CylancePROTECT agent, it stopped responding if any netcore application was running. (EPP-2172)

Fixed in Linux agent version 3.0.1000

There are no fixed issues in this release.

Known issues in the Linux agent

The agent updater proceeds to install the agent and driver (as if there's an update) even though the same version was already installed. The agent continues to run as expected and the unnecessary updates do not continue to occur. (EPP-2874)
After the installation of the agent, if the first agent update is not successful, the updater could not roll back the installation because the installation files cannot be found. (EPP-2726) **Workaround**: After installation, copy the each of the installation packages (.deb or .rpm) for the agent, drivers, and UI to the `/opt/cylance/desktop` directory.
On a SUSE 11 system (SLES 11), after upgrading from 1570 to 1580, attempts to downgrade back to 1570 was not successful. (CHP-8341)
On a SUSE 11 SP4 64-bit system (SLES 11), upgrading the agent may result in the exception `System.TypeInitializationException` appearing multiple times in the log file. (CHP-7916)
On an Ubuntu 14.04 and 16.04 systems, when upgrading from 1570 or 1580 to 1590, and then downgrading from 1590 to 1570 or 1580 results in the agent continuously trying to downgrade to 1570 or 1580. This results in a continuous rollback and failure messages in the agent logs. (EPP-1475, EPP-1477)

On SUSE SLES 11 SP4, if you upgrade from agent 1570/1574 to agent 1580 and then downgrade back to agent 1570/1574, the downgrade is initially successful, but is eventually upgraded back to agent 1580. (CHP-8293)
On Amazon Linux 2, installing the agent on newer kernels is successful, but a "CyProtectDrv: module verification failed: signature and/or required key missing - tainting kernel" error displays because a signature is missing. The agent still runs properly and the error can be ignored. (CHP-7335)

What's new in the CylancePROTECT Desktop agent for macOS

What's new for the macOS agent 3.2.1000

Feature	Description
Background threat detection on-demand scan	Administrators can now initiate a background threat detection scan on demand from the management console. The command can be sent from the Device Details screen for an individual device, or for multiple devices at once from the Devices screen.
Added support for macOS 14 (Sonoma)	The CylancePROTECT Desktop agent for macOS 3.2 now supports devices that are running macOS 14 (Sonoma). You must use this agent version even though previous versions of the agent might continue to run on the device. The supported upgrade path is that you must upgrade to agent 3.2.1000 first, before you upgrade to macOS 14. For example, upgrade the agent to version 3.2.1000 while the device is running macOS 13, then upgrade to macOS 14.

What's new for the macOS agent 3.1.1000

Feature	Description
Added support for macOS 13	The CylancePROTECT Desktop agent 3.1 now supports devices that are running macOS 13 (Ventura). You must upgrade to CylancePROTECT Desktop agent 3.1 on devices that are running macOS 13, even though agent version 3.0 might continue to run on these devices after upgrading to macOS 13.
Custom interval for background threat detection scanning	Administrators can now set a custom interval to run background threat detection scanning from the device policy. The scan interval can be set between 1 and 90 days. The default scan interval is 10 days. Note that increasing the frequency of the scans might impact device performance. You can also start the scan manually from the command line. The date of the last scan for each device is logged in the management console.

What's new for the macOS agent 3.0.1000

Feature	Description
Added support for macOS 12	The CylancePROTECT Desktop agent now supports devices that are running macOS 12 (Monterey).

What's new for the macOS agent 2.1.1594

Item	Description
Apple Mac M1 ARM processor support	The CylancePROTECT Desktop now supports devices that use the Apple Mac M1 ARM processor.

Fixed issues in the macOS agent

Fixed issues in the macOS agent version 3.2.1000

If you tried to uninstall the agent, a “Secure coding is not enabled” error message appeared. (EUS-1546)
When a file in the global quarantine list was detected and blocked, the block action was not reported to the management console if the file was deleted before the agent processed the event. (EPP-1709)
On macOS devices with the M1 chipset, the CylancePROTECT Desktop agent caused a kernel panic and rebooted when you tried to run an Xcode simulator. (EUS-1048)
On macOS devices with the M1 chipset, the CylancePROTECT Desktop agent was slow to shutdown during a device reboot when full disk access was enabled. (EUS-1019)

Fixed issues in the macOS agent version 3.1.1000

The CylancePROTECT Desktop macOS agent did not load proxy auto-configuration (PAC) files properly. (EPP-1978)
When you installed or upgraded to the CylancePROTECT Desktop 3.0.1000 agent on a device running macOS 11 or later, the CyProtectDrvOSX kext was still found on the system, even though it was no longer required. (EPP-2942)

Fixed issues in the macOS agent version 3.0.1000

There are no fixed issues in this release.

Fixed issues in the macOS agent version 2.1.1594

On macOS Big Sur, a kernel panic would intermittently occur when running the agent. This was related to checking if a file is an executable and has been resolved. (CHP-8535, UD-1626)
On macOS Monterey, the agent stopped responding when closing a file when Memory Protection was enabled. (UD-1616)
On different macOS versions, memory usage increased. (EPP-1708)
On macOS Monterey, the CylanceSvc and CyUpdate services would not run. (EPP-1643)
On macOS Big Sur devices, the CylancePROTECT Desktop agent gave multiple Remote Allocation of Memory (OopAllocate) memory protect alerts for osqueryd. (UD-1266)

Known issues in the macOS agent

* When you initiate a background scan from the command line, a warning message appears before the scan starts. The scan starts successfully. (EUS-1467)
On macOS Catalina devices, the Cylance logo might not display on the Cylance UI About page or Installation Token prompt dialog box. (CHP-7509)

CylancePROTECT Mobile release notes

Latest versions of the CylancePROTECT Mobile app

- CylancePROTECT Mobile app for iOS: 2.20.0.3926
- CylancePROTECT Mobile app for Android: 2.20.0.3926

What's new in CylancePROTECT Mobile

Feature	Description	Date added
Use Intune app protection policies with CylancePROTECT Mobile	You can use Microsoft Intune app protection policies with CylancePROTECT Mobile to allow or restrict access to specific Microsoft apps based on the device threat level reported by CylancePROTECT Mobile. For more information, see Use Intune app protection policies with CylancePROTECT Mobile.	March 2024
Add installer sources to the sideload detection safe and restricted lists	You can now exempt specific installer sources from sideload detection and classify specific installer sources as a threat for sideload detection. For more information, see Add an app, certificate, IP address, domain, or installer source to a CylancePROTECT Mobile safe or restricted list.	February 2024
Change to iOS support	This release of the CylancePROTECT Mobile app removes support for iOS 15.	December 2023
Support for the Play Integrity API	The May release of the CylancePROTECT Mobile app adds support for the Play Integrity API for attestation of the app on Android devices. Play Integrity attestation replaces SafetyNet attestation. Older versions of the app will continue to support SafetyNet attestation until Google removes support. To ensure that Play Integrity attestation works as expected, instruct users to update to the latest version of Google Play.	May 2023
Change to Android OS support	The May release of the CylancePROTECT Mobile app removes support for the Android 9 OS.	May 2023
Record of the most recent device scan	The Device Health section of the CylancePROTECT Mobile app will indicate when the most recent scan for threats occurred.	December 2022 (Android) October 2022 (iOS)
Browser support	The CylancePROTECT Mobile app now supports the Firefox and Brave browsers for Android.	December 2022

Feature	Description	Date added
New name for the app	The late July release rebrands the BlackBerry Protect app to the CylancePROTECT Mobile app.	July 2022
Samsung Knox Enhanced Attestation	This release supports the use of Samsung Knox Enhanced Attestation in regular intervals to validate the integrity of users' Samsung devices. Knox Enhanced Attestation is hardware-based and can detect device tampering, rooting, OEM unlock, and IMEI or serial number falsification, in addition to performing app health checks.	July 2022
Enhancements to SMS monitoring for Android devices	This release introduces new options in CylancePROTECT Mobile policies that allow you to specify an age threshold for SMS messages that can be scanned (up to 7 days old), and the ability to obfuscate certain pieces of data that Cylance Endpoint Security collects, including URLs and the email or phone number of the sender. When a malicious URL is detected in a text message, an alert is reported in the management console on the Protection > Protect Mobile Alerts page.	July 2022
Administrator controls for detecting developer mode on Android devices	Previously, the ability to detect developer mode on Android devices was always on and you did not have the option to turn this feature off. In this release, CylancePROTECT Mobile policies now include the option to turn this feature on or off. When developer mode is detected on a device, an alert is reported in the management console on the Protection > Protect Mobile Alerts page.	July 2022

CylancePROTECT Mobile fixed issues

CylancePROTECT Mobile app (all platforms)

If a user deactivated the CylancePROTECT Mobile app, then changed the device language and activated the app again, the text on the activation screen used the original device language instead of the new device language. (UESAPP-3111)

CylancePROTECT Mobile app for Android

If you added an app to the CylancePROTECT Mobile restricted list in the management console, when the app was detected on devices, the user might have received more than one new threat notification. (MTDLIB-1176)
If the Network protection > Wi-Fi security feature was turned off in the app and the user turned it on and selected "Maybe Later" in the permission prompt, the app indicated that a threat was detected. (MTDPLR-19)
When you navigated to a user's device details in the management console and viewed Alerts > Protect Mobile Alerts, if you tried to filter the results to SafetyNet or Play Integrity attesation failure alerts, the results were not filtered and the following error message displayed: "An error occurred. Please try again." (UES-13110)

Some status messages, tooltips, labels, and descriptions in the management console referenced SafetyNet attestation when they should have referenced SafetyNet and Play Integrity attestation. (UES-13010, MTD-7931, MTD-7927)
If the CylancePROTECT Mobile app was installed and activated in the Intune portal on an Android OS 13 device, in the App info, the "Pause app activity if unused" option was greyed out and the user could not turn it off. This prevented the user from turning off battery optimization for the app, and they saw a warning message in the Device Health section that they could not dismiss. (UES-10189)
App configurations that you created from the Cylance console did not register successfully for Android devices with the CylancePROTECT Mobile app version 2.2.0.1381. This issue was fixed by a Cylance Endpoint Security update on March 24 2022. (UES-7516)
For CylancePROTECT Mobile devices configured for Intune integration, if the user did not complete Microsoft Online Device Registration, when the user force closed and reopened the CylancePROTECT Mobile app, the Microsoft Online Device Registration banner with the register link did not display as expected. (UES-7243)
When Play Integrity or SafetyNet attestation failed, the user received a notification on their device even if the CylancePROTECT Mobile policy was not configured to display device notifications for attestation issues. (UESAPP-3962)
In the CylancePROTECT Mobile app, if some device security features were turned off and no device security threats were detected on the device, the text in the Device Health > Device security section of the app displayed in yellow instead of green. (UESAPP-3644)
After a user turned on Wi-Fi protection in the CylancePROTECT Mobile app and granted the required permission, a false “No Wi-Fi connected” threat displayed for a few seconds. (UESAPP-3269)
After a user activated the CylancePROTECT Mobile app, when the user tapped Device Health for the first time, there could be a delay of up to 20 seconds before the UI displayed. (UESAPP-3154)
After a user activated the CylancePROTECT Mobile app and granted permissions for the app to check the security of the Wi-Fi network, for up to 30 seconds, Device Health > Network Protection indicated that network security features were disabled. (UESAPP-3147)
If a user tried to activate the CylancePROTECT Mobile app on a Samsung S20 or S21 device with Android 12 using their activation credentials, the activation failed with the following error: "The specified key does not exist." (UESAPP-2865)
If you removed an app from the CylancePROTECT Mobile safe list or unsafe list, it could take up to 30 minutes for that change to take effect on devices (for example, if an app was removed from the safe list and was considered malicious by the CylancePROTECT cloud services, it could take up to 30 minutes for the CylancePROTECT Mobile app to detect it). If malware detection was turned off on in a CylancePROTECT Mobile policy and you turned it on, it could take up to 30 minutes for the CylancePROTECT Mobile app to start detecting malicious apps. (UESAPP-2547)
If a device was activated on BlackBerry UEM with the Android Enterprise activation type using BlackBerry Secure Connect Plus, when the CylancePROTECT Mobile app was installed in the work space as a required app, a network connection error occurred when the user tried to activate the app. The app did not activate successfully. (UESAPP-2251)

If a user's device was rooted, when the user moved the CylancePROTECT Mobile app from the background to the foreground, a "Threat detected" notification might have displayed on the device. (UESAPP-2210)

CylancePROTECT Mobile app for iOS

If you turned on Unsupported OS in a CylancePROTECT Mobile policy and added OS 16.4.1.(a) to the unsupported list, when the policy was applied to a device, the CylancePROTECT Mobile app stopped responding and closed instead of displaying an alert that the OS was not supported. (UESAPP-4012)
On devices with iOS 16.2, if a user enabled SMS message filtering, the feature was turned off after the user upgraded the app. (UESAPP-3764)
If a user sent the CylancePROTECT Mobile app to the background, then brought it to the foreground again, it could take up to 10 minutes for the app to check the device for threats. (UESAPP-3638)
For CylancePROTECT Mobile devices configured for Intune integration, if a user had not completed the Microsoft Online Device Registration process and snoozed the notification for one hour, the notification did not display again after one hour if the CylancePROTECT Mobile app was not running in the background. The user had to wait for the notification that would display every 24 hours. (UESAPP-2583)
If the CylancePROTECT Mobile app detected more than one threat, after you resolved one of the threats, a notification for a new threat still displayed on the device even though no new threats had been detected. (UESAPP-2553)
When a user tried to deactivate the CylancePROTECT Mobile app, in certain circumstances the deactivation could fail and cause the app to stop responding. (UESAPP-2228)
If a device security threat was detected and resolved, the device security section of the app might have still displayed a threat alert. (UESAPP-2224)
When a user deactivated the CylancePROTECT Mobile app, there was no dialogue to indicate that deactivation was in progress. (UESAPP-2167)
When a user activated the CylancePROTECT Mobile app, for the options under the text "No QR code?", the user had to tap the icon for the option and could not tap the text. (UESAPP-1886)

CylancePROTECT Mobile app for Chrome OS

After activating the CylancePROTECT Mobile app, when the user was prompted to ignore battery optimization settings, a "This setting is not supported" error displayed. The user could close the error and allow the app to run in the background, but a message continued to display in the app reminding the user to allow it to run in the background. (UESAPP-3533)

CylancePROTECT Mobile known issues

CylancePROTECT Mobile app for Android

If you turn off hardware attestation, then turn it on again, the previous attestation state will be reported instead of initiating a new attestation check. (MTD-6839)

On Samsung Galaxy S22 devices or later with Android 13 and the December 2022 security patch, Samsung Knox Enhanced Attestation fails and is reported as a threat in the CylancePROTECT Mobile app. (MTDPLR-21) **Workaround:** Turn off Samsung Knox Enhanced Attestation in the CylancePROTECT Mobile policy assigned to devices until Samsung resolves the issue.
If you configure Intune app protection to work with CylancePROTECT Mobile, when a user opens a protected Microsoft app and follows the prompts to install and activate the CylancePROTECT Mobile app, after the user taps "Launch", the CylancePROTECT Mobile app does not open as expected. (UESAPP-4094) **Workaround:** The user must open the CylancePROTECT Mobile app manually and then return to the protected Microsoft app.
If a user's default device browser is Firefox, after the user enters their activation credentials, the activation process does not start. This is due to a known issue with Firefox. (UESAPP-1804) **Workaround:** Enable the "Open links in app" options in the Firefox settings on the device.
When the CylancePROTECT Mobile app detects a restricted app (an app with a developer certificate that has been added to the malware and sideload detection restricted list in the management console), multiple alerts display in the app instead of a single alert. (UESAPP-1696)

CylancePROTECT Mobile app for iOS

On certain devices, including iPhone 12 Pro Max and iPhone SE 2020 (iOS 15.2), CylancePROTECT Mobile policy changes that are sent from Cylance Endpoint Security to the CylancePROTECT Mobile app might not apply immediately if the app is running in the background. (UESAPP-2433)
False app integrity alerts might occur on iPhone X iOS 14.6 devices. (UESAPP-2421)

CylancePROTECT Mobile app for Chrome OS

If you turn on hardware attestation and set a security patch level for PixelBook devices, an alert is not displayed in the app and management console if a PixelBook Go device does not meet the patch level you specified. (UESAPP-2271)
On certain Chrome OS, after a user enters their activation credentials, the user is not redirected to the CylancePROTECT Mobile app and the activation does not complete successfully. (UESAPP-887) **Workaround:** In the "Open with" prompt, select Protect and Open. If the prompt does not display, click the square with the arrow icon.
When a user scans their QR code to activate the CylancePROTECT Mobile app and taps Continue, the user is not redirected to the CylancePROTECT Mobile app and activation does not complete successfully. (EID-16707) **Workaround:** Reload the browser page.

CylanceOPTICS release notes

What's new in CylanceOPTICS (January 2024)

Feature	Description
CylanceOPTICS agent versions	This release includes the new CylanceOPTICS agent for Windows version 3.3.2311.0. For more information about supported operating systems, see the Cylance Endpoint Security compatibility matrix.
Enhancements to the logic and methods that CylanceOPTICS uses to identify security threats	CylanceOPTICS 3.3 features significant enhancements to the underlying logic and methods that the CylanceOPTICS cloud services and the CylanceOPTICS agent use to identify security threats. These changes include: • Improvements to how the CylanceOPTICS agent collects context-relevant event data for a given detection. • Improved collection and identification of the processes and events that precede a given detection, and of the noteworthy processes and events that follow a given detection. This provides a more detailed and accurate picture of the factors that may have resulted in the detection and of the aftermath of that detection. • Improved data collection methodologies controlled by the CylanceOPTICS cloud services, enabling CylanceOPTICS to stay ahead of a threat landscape that is always evolving. These changes ensure that the agent can collect the most valuable telemetry while also tuning out data that is not relevant.
New sensors	This release of the CylanceOPTICS agent adds three new optional sensors for Windows devices: • COM Object Visibility: Allows the CylanceOPTICS agent to monitor COM objects. • HTTP Visibility: Allows the CylanceOPTICS agent to track Windows HTTP transactions. • Module Load Visibility: Allows the CylanceOPTICS agent to monitor module loads. These sensors require the CylancePROTECT Desktop agent version 3.2 or later. For more information, see CylanceOPTICS optional sensors in the Cylance Endpoint Security Setup content.
Data enrichment for Windows events	Previously, the CylanceOPTICS agent collected the Provider Name, Class, and Event ID facets for Windows Event artifacts. This release adds significant data collection enhancements for Windows Events, with the agent collecting the data defined in the EventData facet of the artifact (for example, this can include ObjectServer, PrivilegeList, Process ID, Process Name, Service, or other facets). For more information, see Data structures that CylanceOPTICS uses to identify threats in the Cylance Endpoint Security Setup content.

What's new in CylanceOPTICS (August 2023)

Feature	Description
Enhancements to advanced query	This release introduces the following enhancements to the advanced query feature in the management console: • As you type the EQL syntax for a query, syntax options and validation messages will display to help you build your query. • You can now schedule the execution of an advanced query for a specific date and time, and you can schedule a query to run on a regular interval. • When you set the scope of your query to specific devices, an icon displays indicating whether each device is online. • New options to filter query results. • When you select a result and open the fly-out menu, you can view additional event data and filter the query results to show matches for one or more facets. • Various UI improvements make it easier for you to add a query, copy a query, and apply and clear zones, devices, and filters for queries. • You can now export the results of a query to a CSV file. For more information, see Create an advanced query in the Cylance Endpoint Security Administration content.

What's new in CylanceOPTICS (April 2023)

Feature	Description
New audit log values for device lockdown configuration in syslog messages	The April update of the CylanceOPTICS cloud services adds new event name values to audit log messages that can be reported to SIEM solutions and syslog servers. The new Event Name fields are associated with the lockdown configuration feature: • LockdownConfigurationAdd • LockdownConfigurationEdit • LockdownConfigurationDelete For more information about audit log events, see the Cylance Syslog Guide.
Lockdown configurations API	The Cylance User API now includes the lockdown configurations API. You can use this API to perform actions on partially locked devices, including: • Getting a list of custom partial lockdown profiles • Creating a custom partial lockdown profile • Updating a custom partial lockdown profile • Deleting a custom partial lockdown profile For more information, see the Cylance User API Guide.

Considerations when upgrading from CylanceOPTICS 2.5.x to 3.x

- For configuration requirements for macOS Big Sur (11.x) or Monterey (12.x), see the setup instructions in the Cylance Endpoint Security Setup Guide.

- If you do not set up a complete MDM profile for the CylanceOPTICS network extension on devices with macOS Big Sur (11.x) or later, data collection might not occur as expected. Verify that you satisfy the configuration requirements for MDM managed devices in the Cylance Endpoint Security Setup Guide.
- BlackBerry recommends installing the latest available version of the CylancePROTECT agent. For more information, see the CylanceOPTICS requirements.
- On macOS devices, after you upgrade the CylanceOPTICS agent you need to restart the device.
- On macOS Catalina, Mojave, and High Sierra devices with the SelfProtection level set to LocalSystem, if you upgrade from CylanceOPTICS agent version 2.5.x to 3.x, the upgrade might not complete successfully. (EDR-7705)

  Workaround: Change the self protection level to LocalAdmin, then update the CylanceOPTICS agent.
- If you upgrade the CylanceOPTICS agent on a CentOS/RHEL 8.0 or 8.1 device, you must restart the device after the upgrade is complete. (EDR-6750)
- Upgrading the CylanceOPTICS agent on Linux from version 2.x to a newer version fails if Security-Enhanced Linux (SELinux) is enabled on the device. (EDR-6264)

  Workaround: Disable SELinux on the device before you upgrade the CylanceOPTICS agent and enable it again after the upgrade is complete.
- When upgrading the CylanceOPTICS agent on Windows, to avoid an issue with the CylanceOPTICS shutdown time taking longer than usual, disable the TDT sensor in the device policy and enable it again after the upgrade is complete. This issue does not occur if you upgrade from CylanceOPTICS agent version 2.5.3010 or from CylanceOPTICS agent 3.0 to a later version. (EDR-6058)

CylanceOPTICS fixed issues

Fixed issues in CylanceOPTICS 3.3

If the API Sensor was enabled in the device policy that was assigned to CylanceOPTICS 3.2.x devices with Windows Server 2016 and CylancePROTECT Desktop agent 3.0.1003 or later, some applications such as Chrome and Powershell might have stopped working. (EDR-10871)
If you ran an advanced query and tried to generate focus data from the results, the focus description that was used to generate the data did not include the correct artifact information. (EDR-9414)
When you viewed the results of an InstaQuery, the count for devices queried and devices responded might not have been accurate. This issue occurred intermittently. (EDR-6523)

Fixed issues in CylanceOPTICS 3.2

If you requested and viewed focus data from the device details page (Assets > Devices) before the event data was loaded to the management console, the resulting focus data did not include any results. (EDRRQ-240)
On Windows 7 devices, if you upgraded to CylanceOPTICS agent 3.1 or later, after you restarted the device the agent did not start as expected. If the user right-clicked the CylancePROTECT icon and clicked System Check, the status of the CyOptics driver was "Not Found". (EDR-14132)

If you created a custom partial lockdown configuration that contained an allowed port value and you assigned it to a CylanceOPTICS device, the allowed port for partial lockdown was not removed when you assigned a different custom configuration. As a result, any ports that you allowed with any partial lockdown configuration remained allowed on the device, regardless of the new configurations that you assigned. (EDR-13243)
In the management console, if you retry a focus data request, the timestamp information is missing. (EDR-10987)
When you scoped an advanced query to specific devices (Search devices > By Device), the Device drop-down listed a maximum of 200 devices. (EDR-10446)
If you deployed a package to CylanceOPTICS devices, when you highlighted a device in the device selection list, you could not see the icon that indicated that the device was online. The color of the icon matched the color of the highlight. (EDR-10224)
When you deployed a package to CylanceOPTICS devices, the status column might have indicated that the job was completed even though the progress bar was not yet full. (EDR-8754)
If you uninstalled the CylanceOPTICS agent using an MDM profile, the network filter CyOpticsESFLoader remained in the system networking on the device. (EDR-7656)
When you viewed focus data and you clicked the path for a file event to create a pivot query, the Search Term field was not pre-populated. (EDR-6785)
On macOS devices, when CylanceOPTICS performed an action on an empty file (for example, a 0 KB .prn file), the event was not included in the datagram file. This is fixed for macOS devices with Big Sur (11.x) or later. (EDR-5545)

Fixed issues in CylanceOPTICS 3.1

If you checked the device details in Optics > Devices after you partially locked or remotely unlocked a device, the device status may not have updated as expected. (EDR-9646)
In some advanced query results, the option to globally quarantine a file was not available. (EDR-9534)
If you cloned an existing package deployment job with a status of created, expired, in progress, or stopped, the device information was not prepopulated in the new package deploy. (EDR-7927)
When you created a package deploy, if you added a device to the request then removed it and tried to add it again, the device did not display on the available devices list. (EDR-7847)
Locking down a macOS device did not close the VNC client on that device. (EDR-6971)
If you ran an InstaQuery for a PowerShellTrace artifact and a Payload or Script Blocked Text facet, the search term was case-sensitive. (EDR-6868)
When you created a pivot query from the focus data timeline view, if the artifact was registry key, the artifact and facet fields were not pre-populated. (EDR-6856)
When you viewed focus data in the table view for a registry key artifact, the name and path were not correct. If you created a pivot query, you did not get any results. (EDR-6855)

In a focus view, the link to clone a pivot query did not work. (EDR-6786)
On macOS Mojave and Catalina, downgrading the CylanceOPTICS agent might have resulted in the lockdown feature not working as expected. (EDR-5735)

CylanceOPTICS known issues

Due to a defect in macOS Ventura 13.0.0, if the CylanceOPTICS agent is installed on a device with macOS 13.0.0 or a CylanceOPTICS device is upgraded to macOS 13.0.0, the CylanceOPTICS agent may not be able to detect events. (EDR-14879) **Workaround:** To prevent this issue from occurring, install the agent on macOS Ventura 13.0.1 or later or upgrade directly to macOS Ventura 13.0.1 or later instead of 13.0.0. If you upgrade from 13.0.0 to 13.0.1 or later, remove the agent and install it again. If installing on 13.0.1 or later or upgrading to 13.0.1 or later is not possible at this time, remove full disk access for CyOptics and CyOpticsESFLoader then add full disk access for both again and restart the device.
When you try to unlock a partially locked device from the management console, it may not unlock as expected. This issue occurs intermittently. (EDR-9690) **Workaround:** Try to unlock the device again from the management console (Select Action > Unlock device), or use the unlock key.
If you try to download a large file from InstaQuery results by clicking the Request File Download button, the request might not complete as expected (the button does not change to "Download File"). (EDR-7702)
When you view the detection details for an event and you request a file download for an instigating process or target file source, the status of the download changes back to "Request File Download" instead of "Download File". (EDR-7007)
The refract package for browser history that is available in the management console does not collect the expected data on Linux devices. (EDR-6917)
If you view the threats and activities for a device and you request data for an event, the focus view status remains at "Data Pending" indefinitely instead of updating to "View Data". (EDR-6779) **Workaround:** View another tab and return to the device's threats and activities.
When you view the status of a package deploy job and you filter the results by name, the operator displays as "Equals" even though it works as "Contains", and the filter is case sensitive. (EDR-6689)

CylanceGATEWAY release notes

What's new in the management console

Feature	Description	Date added
Change to network anomaly detection of users' traffic patterns	CylanceGATEWAY has deprecated support for behavioral risk detections based on unusual user behavior such as upload volume and download volume that is not consistent with past behavior.	January 2024
DGA detection	CylanceGATEWAY now proactively detects domains that have been created using a Domain Generation Algorithm (DGA) when users attempt to access the domain. Identified DGA events are labelled as Zero Day Detection and categorized as a Dynamic Risk and subcategorized as DGA. The anomaly detection threat events are sent to the Alerts view, the Events page, and the SIEM solution or syslog server, if configured. This feature provides a continued evolution of CylanceGATEWAY network protection capabilities.	November 2023
Safe Mode enhancements	CylanceGATEWAY now extends Machine Learning-based network protection to Safe Mode. In addition to applying the tenant's ACL rules, the Network Protection settings applied to Safe Mode have, therefore, expanded from Destination Reputation to include the following types: • DNS Tunneling • Zero Day This feature provides additional protection to endpoints against newly emerging network threats and malicious destinations based on the network protection settings that you specify.	November 2023
Control the network traffic detections that are sent to the Alerts view	On the Network Protection settings screen, you can now specify the following detections that you want to enable and be displayed in the Alerts view: • Signature detections: Blocked and allowed events • Destination reputation: Blocked and allowed events based on the minimum risk level that you set • DNS tunneling: Based on the minimum risk level that you set • Zero Day: Based on the minimum risk level that you set Blocked and allowed ACL events are not shared to the Alerts view. This feature introduces a more granular control over the events that are shared to the Alerts view. For more information, see Configure network protection settings in the Cylance Endpoint Security Setup content.	November 2023

Feature	Description	Date added
Evaluate the risk level of a network destination	You can use the management console to evaluate the risk level and identify the category and subcategory of a network destination, as analyzed, and determined by the CylanceGATEWAY cloud services. This feature provides you with insight into how CylanceGATEWAY would classify and assign a risk level to a destination. For example, when you configure your access control list (ACL) rules and network protection settings to allow or block destinations and you want to know how a specific destination might be categorized, you can now safely determine the category and risk level that CylanceGATEWAY has assigned to the destination. For more information, see Evaluate the risk level of a network destination page in the Cylance Endpoint Security Setup content.	November 2023
Domain classification enhancements	CylanceGATEWAY uses Machine Learning that applies categorization to previously uncategorized English destinations. This feature has been expanded to now classify previously uncategorized French, German, Italian, and Spanish-language web destinations (for example, General Interest – Business or Security Risk). For more information, see Destination content categories page in the Cylance Endpoint Security Setup content.	November 2023
Event Details page enhancements	• **DNS request and response**: If the Events page displays a DNS event, the Events Details page will display the DNS request and all the response details for the event. This feature allows you to view the entire path that is associated with a DNS query. DNS request and responses are sent to the Alerts view and the SIEM solution or syslog server, if configured. • **Safe Mode telemetry enhancements**: The Events Details page now displays additional metadata; process ID (PID) and process name (Pathname) to help administrators and SOC Analysts in their threat hunting and post incident review. The PID and pathname are sent to the Alerts view and the SIEM solution or syslog server, if configured. For more information, see Viewing the Event Details in the Cylance Endpoint Security Administration content.	November 2023

Feature	Description	Date added
Support for multiple private network configurations	You can now configure CylanceGATEWAY to allow access to resources on more than one private network (for example, segments, data centers, and VPCs) both in on-premises and cloud environments. You can view the CylanceGATEWAY Connectors that are associated with each specified Connector Group. This feature allows you to deploy multiple CylanceGATEWAY Connectors from one Cylance Endpoint Security tenant and provides an aggregated view of the connectors for each private network. **UI updates** • The left “Network Routing” navigation menu has been renamed to “Connector Groups”. • The “Health Check” and “Source IP restriction” configuration screens have been moved to “Connector Groups". • In the "Gateway Connectors" navigation menu, the “Tunnel”, “DNS”, and “HTTP” columns have been combined into the “Health Check Status” column. You can click the Health Check Status column to view additional connector information (for example, whether a tunnel is established and the DNS server IP address).	July 2023
Improved control of network traffic settings	The updated Network Protections settings introduce more granular control over the detection and protection mode of features of CylanceGATEWAY, the respective details that you want to have reported and displayed in the Network Events screen, and the level of details shared to your integrated SIEM solution or syslog server, if configured. • The current "Network Protection" settings have moved to the **Protect** tab. The Network protection action “Enable intrusion protection” has been renamed to “Enable Signature detection”. • The new **Report** tab allows you to specify the details that will appear in the Network Events page as detections or normal traffic. • The new **Share** tab allows you to specify the details that are sent to the SIEM solution or syslog server, if configured. By default, blocked detections are always sent. Optionally, you can choose to also send allowed detections. For more information, see Configuring network protection in the Cylance Endpoint Security Setup content.	July 2023

Feature	Description	Date added

Enhancements	On the CylanceGATEWAY Events page,
	• **New category**: Previously the "Security Risk" category was applied as both a content category for destinations that were deemed non-malicious (for example, destinations that teach about malware), as well as an anomaly category for destinations that are considered malicious (for example, destinations that distribute malware). Now when CylanceGATEWAY detects an IP reputation, the IP reputation will be categorized as one of the following:
	  • **Dynamic Risk**: This new category is applied to destinations that are identified to contain potentially malicious threats by using a combination of ML models and IP Reputation database which continuously changes to add or remove destination entries.
	  • **Security Risk**: This category is now applied only as a content category to non-malicious destinations.
	• **New BlackBerry source IP address filter capability**: You can now filter events based on the CylanceGATEWAY tunnel IP address. The "BlackBerry source IP" identifies the tunnel IP address users used to access external destinations. This feature provides administrators with added visibility in the tunnel that was used when an event has occurred.
		July 2023

Enable Split DNS	In the Gateway Service policy, you can now enable Split DNS after Split tunneling is enabled. For more information on split DNS tunneling, see "Split tunneling enhancements" below.	June 2023
HTTP content logging	In the ACL rules, you can now specify whether network events should include unencrypted, plain-text HTTP connection data. When enabled, a summary of the request and response details of an event are displayed in the Events Details page. The Events details page displays the first three HTTP events of the total events. You have the option to view all the events and the details that are associated with each one. This feature allows unencrypted HTTP network traffic to be reviewed and analyzed more deeply while further enabling threat hunting.	June 2023

Feature	Description	Date added
Safe Mode DNS protection support on Windows	In the Gateway Service policy, you can configure users to use Safe Mode. This feature extends the tenant's ACL rules and endpoint protection for devices when Work Mode is not enabled ensuring that devices are always protected. With Safe Mode, CylanceGATEWAY blocks users from accessing potentially malicious destinations and enforces acceptable use policy (AUP) by intercepting DNS requests. The CylanceGATEWAY Cloud services evaluate each DNS query against the configured ACL rules and network protection settings, and then instructs the agent to allow or block the request in real time. If allowed, the network DNS query is allowed to complete over the bearer network. Otherwise, the CylanceGATEWAY agent overrides the normal response and prevents access. When enabled, Safe Mode automatically takes effect when Work Mode is disabled. Enabling Safe Mode does not prevent users from enabling or disabling Work Mode, if the users' policy allows such operations. Safe Mode events appear in the CylanceGATEWAY Events screen and are sent to the SIEM solution or syslog server, if configured. This feature is not supported in environments that use secure DNS with DoT (DNS-over-TLS) and DoH (DNS-over-HTTPS) protocols. DNS queries sent using DoT or DoH cannot be viewed by CylanceGATEWAY. This feature is supported on CylanceGATEWAY agent for Windows version 2.8 or later. For more information, see the Gateway Service policy parameters in the Cylance Endpoint Security Setup content.	June 2023
OS-specific ACL support	In the ACL rules, you can create rules and specify which OS that the ACL rule applies to must match. This feature allows you to unify the ACL rules. For example, you have content sensitive resources that you only want desktop devices (macOS and Windows) to access. In this scenario, your ACL rule would specify the desktop devices which are allowed access to the resource. For more information, see the ACL parameters in the Cylance Endpoint Security Setup content.	June 2023

Feature	Description	Date added
Split tunneling enhancements	Now when you enable split tunneling, split DNS queries allow lookups for the domains that are listed in the Private Network > DNS > Forward Lookup Zone configuration to be performed through the tunnel where network access controls are applied. All other DNS lookups are performed using your local DNS server. Android and 64-bit Chromebook devices do not support split DNS queries and the DNS lookups are performed through the tunnel. This feature allows you to further ensure user traffic privacy and geographical locality of the DNS queries, enhancing the Split Routing feature of Gateway. Split DNS is disabled by default. If you enabled Safe Mode, DNS traffic that does not use the Gateway tunnel is protected by Safe Mode. For more information, see the Gateway Service policy parameters in the Cylance Endpoint Security Setup content.	June 2023
Enhancements	On the CylanceGATEWAY Events page, • **UI Update**: The “Platform” column has been renamed to “OS”. On the Events Details page, • **UI Update**: The “Platform” column has been renamed to “OS”.	June 2023

CylanceGATEWAY component versions

- CylanceGATEWAY Connector version 2.10.0.938
- CylanceGATEWAY agent for Windows version 2.9.0.7
- CylanceGATEWAY agent for macOS version 2.9.14

To download the agent, go to the BlackBerry Website and scroll down to the Download CylanceGATEWAY section.

What's new in CylanceGATEWAY Connector

Feature	Description	Release date and version
Amazon Web Services (AWS) connector installation enhancements	This release of the CylanceGATEWAY Connector provides the CylanceGATEWAY Connector AMI image in AWS Marketplace. This reduces the number of tasks and time for you to set up the connector (for example, you do not need to import the file to the AWS environment, which can take up to 30 minutes to complete). For more information, see Setting up the CylanceGATEWAY Connector in the Cylance Endpoint Security Setup content. For a walkthrough on how to install the connector, see Install the CylanceGATEWAY Connector to an AWS environment.	April 2024 2.10.0.938
Support for future in-place upgrade of the CylanceGATEWAY Connector	You can perform future in-place upgrades of your CylanceGATEWAY Connector and your configurations will be retained. This feature is supported on CylanceGATEWAY Connector version 2.9 or later. This feature provides enhanced user experience in reducing the time required to upgrade the connector. **Note:** The DEB file for the in-place upgrade will be available for download from *my*Account with the next release of the CylanceGATEWAY Connector that is currently scheduled to be released in early 2024. For more information, see Update a CylanceGATEWAY Connector in the Cylance Endpoint Security Setup content.	November 2023 2.9.0.895
Verify the CylanceGATEWAY Connector connectivity	Administrators can use a command line tool to initiate a connectivity test to verify the connection between the CylanceGATEWAY Connector and BlackBerry Infrastructure when the connector is enrolled, but its tunnel is not connected to the BlackBerry Infrastructure. This feature verifies whether the UDP packets sent from your private network have reached the BlackBerry Infrastructure and the UDP packets sent from the BlackBerry Infrastructure have been received by your private network. For more information, see Update a CylanceGATEWAY Connector in the Cylance Endpoint Security Setup content.	November 2023 2.9.0.895

What's new in CylanceGATEWAY agent for macOS

Feature	Description	Release date and version
Activation enhancements	You can now include the custom domain when the installation process of the CylanceGATEWAY agent is controlled by enterprise device management tools, requiring users to only enter their username and password to activate the agent. This feature provides enhanced user experience by allowing the agent to be activated with minimal user interaction. For more information, see Installing the CylanceGATEWAY agent in the Cylance Endpoint Security Setup content.	November 2023 2.9.14
Bug fixes	Bug fixes that are described in the CylanceGATEWAY fixed issues section.	August 2023 2.8.14

What's new in CylanceGATEWAY agent for Windows

Feature	Description	Release date and version
Activation enhancements	You can now include the custom domain when the installation process of the CylanceGATEWAY agent is controlled by enterprise device management tools, requiring users to only enter their username and password to activate the agent. This feature provides enhanced user experience by allowing the agent to be activated with minimal user interaction. For more information, see Installing the CylanceGATEWAY agent in the Cylance Endpoint Security Setup content.	November 2023 2.9.0.7
Enhancements to “Automatically start CylanceGATEWAY when user signs in” and “Enable Work Mode Automatically” and Safe Mode policy settings	In the Gateway Service policy, when you configure the CylanceGATEWAY agent to automatically start and enable Work mode or enable Safe Mode, the agent is minimized in the system tray when it launches. This feature does not prevent users from opening the agent and enabling or disabling Work Mode after the agent starts or close the agent.	November 2023 2.9.0.7

CylanceGATEWAY fixed issues

Fixed issues in BlackBerry UEM Connector

In environments with the following policy settings, the first time that Android users tried to Enable Work Mode the attempt failed. (BIG-11454)

- UEM policy settings
  - Force always-on VPN
  - Force work apps to only use VPN
- Gateway Service policy setting: Allow Gateway to run only if the device is managed by BlackBerry UEM or Microsoft Intune.

Fixed issues in the CylanceGATEWAY agent for macOS versions 2.9.14

After users upgraded the CylanceGATEWAY agent for macOS or Windows to version 2.8.14 or 2.8.0.10, respectively, and then tried to enable Work Mode, Work Mode was not enabled if the following policy settings were configured:

- Tunnel Reauthentication: Enabled
- Allow authentication reuse: Disabled
- Grace period: Enabled

(BIG-11739)

Fixed issues in the CylanceGATEWAY agent for macOS versions 2.8.14

When users cancelled the prompt to reauthenticate the CylanceGATEWAY agent, and then tried to enable Work Mode, Work Mode was not enabled. (BIG-11463)

CylanceGATEWAY known issues

Items marked with an asterisk (*) are new for this release.

Access control list (ACL)

In some scenarios, an ACL rule might be expected to block a connection to a destination, but it isn't when the following combined ACL properties are used to create the rule. (BIG-6511)

Consider the following scenario, this ACL rule will allow users to access to *.example.com when the following ACL properties are specified because the DNS request for http://example.com will be resolved to an IP address (for example, 172.16.10.55) and the request to the IP address on port 80 is not blocked.

In the **Action** section,

- The Action drop-down list displays **Block**.
- The **Ignore port** check box is cleared.

In the **Destination** section,

- The **Target** dropdown list displays **Matches any**.
- In the **Address and Ports** field, you entered `*.example.com` with port `80`.

To block access to the destination in the above scenario, best practice is to enter the FQDN without a wildcard or enter the FQDN with a wildcard and not specify a port number. To have this rule block access to the destination as expected, you must update the ACL rule to one of the following:

Block destination	ACL properties
Specify the destination FQDN and port number. In this rule, when the DNS resolves the FQDN name, the resolved IP address is included in the rule.	In the **Action** section, • The Action drop-down list displays **Block**. • The **Ignore port** check box is cleared. In the **Destination** section, • The **Target** dropdown list displays **Matches any**. • In the **Address and Ports** field, you entered `example.com` with port `80`.
Specify the destination FQDN with a wildcard, no port number.	In the **Action** section, • The Action drop-down list displays **Block**. • The **Ignore port** check box is selected. In the **Destination** section, • The **Target** dropdown list displays **Does not match**. • In the **Address and Ports** field, you entered `http://*.example.com`.

The ACL tab is not displayed in the Cylance Endpoint Security console immediately after CylanceGATEWAY is enabled for the tenant. (BIG-7059)

Workaround: Log out of the Cylance Endpoint Security console, and log in again.

Network connections

On macOS devices when split tunneling is enabled and a DNS query is made for an unqualified hostname, the DNS suffixes may not be applied or used as defined in Settings > Network > Client DNS. (BIG-11180)

Workaround: Complete one of the following:

- Disable split tunneling and users use CylanceGATEWAY to access network resources.
- Instruct users to use the FDQN to access network resources.

When Windows devices are configured to use Safe Mode and Work Mode is not enabled, if third-party solutions that control DNS such as VPN are enabled, they may not work as expected. When enabled, Safe mode intercepts and evaluates all DNS queries and may have conflicts with other solutions that also control DNS. For more information on Safe Mode, see CylanceGATEWAY release notes. (BIG-11098)

If the component that is handling active connections through the CylanceGATEWAY Connector is restarted within the BlackBerry Infrastructure, the number of active connections for the connector may not return to zero when the connector is disabled. (BIG-8614)

Restricted apps can't open loopback sockets when "Block network traffic from restricted apps" is set to "No" in the CylanceGATEWAY service policy, for Windows devices. (BIG-7593)

The Intel Killer Prioritization Engine may drop CylanceGATEWAY traffic. (BIG-5527)

Workaround: Give BlackBerryGatewayService.exe a priority of "1" in the Killer Prioritization Engine console.

If a device's local network IP range (for example, a home Wi-Fi network) overlaps with the customer's private network, CylanceGATEWAY work mode does not allow access to the private network resources for the IPs that fall in the overlap range. For example, if a user's home Wi-Fi network range uses 10.0.0.0/24 and the customer's private network uses 10.0.0.0/8, the user will not be able to access 10.0.0.100 on the private network as it falls under 10.0.0.0/24 and will be routed to the local network. (BIG-5389)

Workaround: Complete one of the following actions:

- User: If the user can configure their local network, the user could change the local network IP range to a private IP range that does not conflict with the customer's private network IP range.
- CylanceGATEWAY administrators: Create and assign a CylanceGATEWAY service policy to the specific user. In the policy, enable split tunneling and add a CIDR address of 0.0.0.0/0 and the IP range of the local network. **Note**: The local network IP range must be added as more specific CIDR addresses (for example, for the local network of 10.0.0.0/24, add 10.0.0.0/25 and 10.0.0.128/25).

BlackBerry UEM Connector

After upgrading to CylanceGATEWAY agent for Windows version 2.8.0.9, DNS tunneling does not enable split DNS when a Group Policy Object (GPO) that sets a DNS name resolution policy table (NRPT) or an empty NRPT exists. When split DNS is not enabled, all DNS lookups are performed through the tunnel. (BIG-11032)

To confirm if a GPO exists, verify whether the Windows registry key "DnsPolicyConfig" is present at `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient\`

After you connect the Cylance Endpoint Security to your BlackBerry UEM Cloud instance, the status of the BlackBerry UEM Connector remains at "In progress". (UES-12931)

Workaround: Refresh the Connectors screen.

On iOS devices that are running CylancePROTECT Mobile app version 2.12.0.3252 or later and BlackBerry UEM Client version earlier than 12.47.3265, and the UEM Client is updated to 12.47.3265 or later the BlackBerry Infrastructure identifies the device as a new activation. (UESAPP-3841)

Workaround: Deactivate and reactivate the CylancePROTECT Mobile app.

Device

* Windows users might experience notifications that rapidly appear and disappear when they attempt to enable Work Mode. Work Mode cannot be enabled. (BIG-11432)

Workaround: The Windows Management Instrumentation (WMI) cannot be accessed or it is corrupt. Repair the WMI. For more information, see KB 112135.

If Work Mode is enabled when the CylancePROTECT Mobile app for iOS updates, a "CylanceGATEWAY is disconnected" message is displayed and users are unable to connect to CylanceGATEWAY. (BIG-8649)

Workaround: Start the CylancePROTECT Mobile app or tap the pop-up message.

When you try to reauthenticate the CylanceGATEWAY agent, you might receive a "Sign-in failed" error. (EID-19203)

Workaround: Temporarily change your default browser or clear the browser cache.

Windows users only receive the Connection Blocked notification popup message the first time they try to access a blocked website. (BIG-8578)

When environments are configured for device posture validation, macOS users receive an error message when they try to enable work mode if the CylancePROTECT Mobile app is installed but not activated. The CylanceGATEWAY agent log file logs a 403 and the following error message: "error":"NotEntitled","detail":"Endpoint requires protect". (BIG-7848)

Workaround: Complete the following steps:

1. Make sure that the CylancePROTECT Mobile app is installed and activated.
2. Close and open the CylanceGATEWAY agent.
3. Click **Enable Work Mode**.

Users may experience connectivity issues when the CylanceGATEWAY agent is installed on a computer running Windows Subsystem for Linux (WSL) due to a known issue where WSL does not accommodate the MTU of the network interfaces in Windows. (BIG-5509)

Workaround: Users with WSL2 can work around this issue using the following commands.

1. Check the MTU WSL2 assigned to the (virtual) "eth0" interface. Note the 1500.

```
$ ip link show dev eth0
6: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode
 DEFAULT group default qlen 1000
link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
```

2. As root in WSL2, set the MTU to match that of CylanceGATEWAY's IPv4 tunnel interface.

```
$ sudo ip link set dev eth0 mtu \
 $(powershell.exe -Command \
   '(Get-NetIPInterface -InterfaceAlias "BlackBerry Gateway" -AddressFamily
 IPv4).NlMtu' \
   |grep -m1 -oE '[0-9]+')
```

3. Confirm that the MTU was changed. Note the 1420.

```
$ ip link show dev eth0
6: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1420 qdisc mq state UP mode
 DEFAULT group default qlen 1000
link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
```

CylanceAVERT release notes

What's new in CylanceAVERT 1.2 (April 2023)

Feature	Description
Support for keyword dictionary	You can now upload a keyword dictionary when creating a data type in this release of CylanceAVERT. A keyword dictionary is a text file that contains all of the keywords for an information protection data type. All keywords in a keyword dictionary must be entered on a separate line in the text file. For more information, see Add a data type in the setup guide.
Alerts view integration	CylanceAVERT alerts can now be surfaced in the Alerts view of the Cylance Endpoint Security console. For more information, see View and manage aggregated alerts in the administration guide.
CylanceAVERT policy enhancements	You can now view if an assigned user policy has been applied to that user and their devices by selecting the user in the Cylance Endpoint Security console. For more information, see View CylanceAVERT user details in the Administration guide.
Data collection enhancements	Non-ASCII filenames are now valid in evidence upload headers.
Dashboard enhancements	You can now select the CylanceAVERT custom dashboard when you are adding a new dashboard. The CylanceAVERTcustom dashboard includes all of the supported CylanceAVERT widgets. This release adds the "Evidence Locker files by date added" dashboard widget.
Support for partially analyzed files	This release adds the following support for partially analyzed files: • You can use the Partially Analyzed Files view to view a list of files that have been partially analyzed and no sensitive information was detected. The file will display in this view with an alert stating that the file was only partially analyzed. • If a file is partially analyzed and sensitive information is detected, it will be treated the same as a fully analyzed file and will display in the File Inventory, Events view, and Evidence Locker. However, an icon displays beside the file in the tables and detailed views with an alert stating that the file was only partially analyzed.
File inventory enhancements	You can now group files in the file inventory based on the following parameters: • Group by users • Group by devices • Group by data types Using these group parameters will display the users, devices, or data types name as well as the number of sensitive files associated with that group in the file inventory. This list is sorted by the number of sensitive files in descending order. You can click on the users, devices, or data types name to view detailed information about the sensitive files.

What's new in CylanceAVERT 1.0 (Janurary 2023)

Feature	Description
Sensitive data scanning	CylanceAVERT can scan files uploaded to USB drives, internet browsers, and email attachments, as well as scan the body content of an email message for company data that the administrator defined as sensitive in the information protection policies. An email notification will be sent for data exfiltration events.
Information protection policies	Administrators can specify the conditions that must be met to trigger the policy violation, the allowed domains for the policy, and the actions to take when a policy has been violated. See Information Protection in the BlackBerry Avert Administration and Overview Guide for more information.
CylanceAVERT events	When the conditions are met to trigger a policy violation, information about that data exfiltration event display in the CylanceAVERT events view. The events view shows detailed information about the event including the data and time of the event, the location that the file was exfiltrated to, the number of policies that were violated, and the user of the device where the event occurred. See BlackBerry Avert Events in the BlackBerry Avert Administration and Overview guide for more information.
Information protection settings	Administrators can use the information protection settings to configure the sensitive data that they want to monitor for by adding templates and data types to use in an information protection policy. Administrators can also define the browser and email domains that will be allowed and trusted, manage the evidence that they want to collect for data exfiltration events, and specify how long the evidence should be available. Specified email addresses can also be sent notifications of data exfiltration events. See Information protection settings in the BlackBerry Avert Administration and Overview guide for more information.
File inventory	The CylanceAVERT file inventory creates a record of all the sensitive files in an organization through a file trawling process. See View the file Inventory to identify sensitive files in the Cylance Endpoint Security Administration Guide for more information.
Evidence locker	Administrators can use the evidence locker to view details of the files that have been involved in exfiltration events and download the files to their local storage for auditing purposes. See Use the evidence locker to view exfiltration event details in the Cylance Endpoint Security Administration Guide for more information.

CylanceAVERT fixed issues

Fixed issues in CylanceAVERT 1.2

The Custom Time function on the "Information Exfiltration Events" widget was still usable when the function was turned off. (DLP-7663)

Read-only users will now see "No permission" when they are viewing information protection widgets that they are not authorized to see. (DLP-7489)
If you clicked on some items on the Data Types tab for the "Top exfiltration events by category" widget, you were redirected to an empty events table. (DLP-7603)
If you clicked on a removable media device from the "Top Exfiltration Events by Location" widget, you were redirected to an empty events table. (DLP-7294)

Fixed issues in CylanceAVERT 1.0

After you saved an information protection policy, you were redirected to the Cylance Endpoint Security dashboard page. (DLP-6573)
The information protection user and devices policies are now applied every hour, instead of every 24 hours. (DLP-6102)
Only domains with 2 or 3 characters (for example .ca or .com) were accepted when adding allowed domains in the information protection settings. (DLP-6097)
The file inventory will now only detect and display files that include sensitive data types that were specified in the information protection policies, instead of all of the sensitive files on the endpoint. This will reduce the number of sensitive files in the file inventory. (DLP-5978)
The CylanceAVERT icon on the management console menu bar was replaced with a question mark on some occasions. (DLP-5549)

CylanceAVERT known issues

If a user that has not been added to Cylance Endpoint Security logs in to a computer that has CylanceAVERT installed, the user will be automatically added to Cylance Endpoint Security.
If a user attaches a sensitive file to an email message in Gmail and cancels the email message before sending it, an exfiltration event will still be triggered because Google will upload the file to a web server regardless of the email that is being sent.
If a user quits the CylanceAVERT app from the Windows system tray, they will not receive a Windows notification when an exfiltration event occurs.
If a Microsoft Outlook personal folder file (.pst) is stored in a network drive, CylanceAVERT will cause your desktop to shut down or restart unexpectedly (BSOD). (DLP-8698) **Workaround**: The .pst file should be moved to a location on the desktop.
Filtering predefined templates does not display the proper results. (DLP-8285)
CylanceAVERT does not support local users (non Active Directory users). (DLP-8262)

The Custom Time function on the "Information Exfiltration Events" widget is still usable when the function is disabled. (DLP-7663)
The following are known issues that relate to widgets: • If you click on some items on the Data Types tab for the "Top exfiltration events by category" widget, you will be redirected to an empty events table. (DLP-7603) • If you click on an removable media device from the "Top Exfiltration Events by Location" widget, you will be redirected to an empty events table. (DLP-7294)
During an exfiltration event involving a USB drive, the temporary copy of the sensitive file is a different size than the original file. (DLP-7494)
If CylanceAVERT is reinstalled on an endpoint, the device information displays the incorrect enrollment date and time. (DLP-7278)
In Firefox, developer tools are disabled. (DLP-6302)
If a user sets a USB or shared folder as the default location for downloads in a browser, the user may receive an exfiltration event notification even if the location where the file will be saved has not been specified. This is due to the browser creating a temp file on the USB or shared folder. (DLP-5399) **Workaround:** Do not configure a USB device or a shared folder as the default location for all browser downloads. For example, in Chrome, do the following: **1.** Open Chrome browser. **2.** In the search bar, type *chrome://settings/downloads*. **3.** Under the Location section, click "Change" and choose a location that is not a USB device or shared folder.
CylanceAVERT does not support directly synchronizing with Microsoft Entra ID Active Directory for user onboarding. As of the 1.0 beta release, CylanceAVERT only supports user onboarding using on-premises Active Directory through the BlackBerry Connectivity Node. (DLP-5366)
A custom data type cannot be deleted if it is used in an information protection policy. (DLP-5319)
If policies are assigned to a user, and then all of those policies are removed, the user will be deleted from CylanceAVERT. (DLP-5253)
You will receive an error when you check the access status of a file with a path longer than 260 characters. (DLP-5050)
The CylanceAVERT extension for Google Chrome is not immediately added after CylanceAVERT is installed. CylanceAVERT will prompt you to close the Chrome browser during installation. (DLP-2182)
When an administrator deletes a file from the Evidence Locker, they cannot see that the files have been removed until the file service updates the Evidence Locker. This can take up to 24 hours to complete. UI enhancements are planned for a future release to communicate this to the administrator when files are deleted. (DLP-2115)
Sensitive data is not detected when it is used in the file name. (DLP-1221)

Legal notice

WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada