Cylance Endpoint Security

Release Notes

Contents

Cylance Endpoint Security product updates

The latest releases of the Cylance Endpoint Security products are listed in the following table. For information about previous releases, refer to KB89592.

Product	Latest release
Management console and platform services	January 2023
CylancePROTECT Desktop	January 2023
CylancePROTECT Mobile	February 2023
CylanceOPTICS	December 2022
CylanceGATEWAY	January 2023
CylanceAVERT	January 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
Administrator controls for discovery of devices not protected by CylancePROTECT Desktop	Previously, the discovery of devices not protected by CylancePROTECT Desktop was enabled and you did not have the option to disable it. In this release, the management console now includes the option to enable or disable this feature. If you enable the feature, you can discover unprotected devices in your environment for your Microsoft Azure Active Directory, Microsoft Active Directory, and LDAP directory connections. When the feature is enabled, all of the known devices that are not protected by CylancePROTECT Desktop are displayed on the Assets > Unprotected Devices page. Enabling or disabling this feature applies to all of the directory connections that you have connected to Cylance Endpoint Security. For more information, see Discover unprotected devices in the Cylance Endpoint Security Administration content.	Jan 2023
Default authentication	To enhance security, the default authenticator for all apps and services except the Cylance console, CylanceGATEWAY agent, and CylancePROTECT Mobile app has been changed from Enterprise password to Deny authentication. Users that do not have an authentication policy assigned to them are presented with an error message when they try to access apps or services and cannot sign in.	Dec 2022
FIDO authenticator	You can now add FIDO as an authenticator in authentication policies. Users can register one or more FIDO2 devices during sign in and use them to verify their identity.	Dec 2022
Identify devices not protected by CylancePROTECT Desktop	The new Unprotected Devices page (Assets > Unprotected Devices) displays a list of known devices that are not protected by CylancePROTECT Desktop. Administrators can export the device list and take action to protect those devices and their network from potential threats. This feature requires BlackBerry Connectivity Node 2.12.1 or later. For more information, see Discover unprotected devices in the Cylance Endpoint Security Administration content.	Oct 2022
BlackBerry Connectivity Node enhancements	The BlackBerry Connectivity Node now supports identifying devices that are not protected by CylancePROTECT Desktop.	Oct 2022

Feature	Description	Date added
New SAML and Deny authenticators and skip OTP option	Cylance Endpoint Security now supports integration with third-party IDPs that support SAML (Azure, Okta, Ping Identity) for use in authentication policies. Administrators can migrate existing SAML configurations from Custom Authentication settings to the new Enhanced Authentication framework. A new a “Deny” authenticator can be added to authentication policies to explicitly deny authentication to a product or service. During authentication, if the Deny Authenticator is found, authentication will be rejected for the user and an error message is presented. Administrators can allow users to skip OTP setup for a specified number of times without losing access to the console. Any existing polices that include the one-time password authenticator will automatically use the default setting of zero skips allowed. For more information, see Add an authenticator in the Cylance Endpoint Security Setup content.	August 2022

Feature	Description	Date added
Hide application secrets for custom app integrations with the Cylance User API	Cylance Endpoint Security supports integration with third-party programs using the Cylance User API, a set of RESTful APIs. This allows your organization to programmatically manage Cylance Endpoint Security settings and configurations. Administrators can customize integration settings to control which API privileges a user has. For security, an API user needs an application ID and an application secret that you generate when you add a custom application in the management console. A security enhancement has been introduced for existing Cylance Endpoint Security tenants. Users with the Administrator role can enable a new feature that permanently removes application secrets from the management console after they are generated, ensuring that they cannot be viewed by any users with access to the Cylance console. If you enable this feature in Settings > Integrations, when an administrator generates or regenerates an application secret, it will display only until the administrator dismisses the dialogue or navigates away from the screen. The app secret will not display in the list. To remove your existing application secrets and enable this behavior, you can expand Improved Security Available and click Remove Secret. After you enable the feature, any application secrets that were generated previously will no longer be available to view. You should record existing application secrets before you enable this feature. You cannot revert to the previous behavior that exposes application secrets in the console. You can generate new application IDs and secrets as necessary. For new Cylance Endpoint Security tenants created after July 2022, this feature is enabled by default. For more information, see Enable access to the Cylance User API in the Cylance Endpoint Security Administration content.	July 2022
Enhanced authentication sign in	The Cylance console now provides enhanced authentication capabilities, such as local multifactor authentication via one-time password, as well as more granular authentication policies and policy assignment for administrators or groups of administrators. You can also create authentication policies for your tenant to specify the default authentication requirements users must complete to sign in to the Cylance console, and to activate the CylancePROTECT Mobile app or CylanceGATEWAY desktop agent. The password pop-up screen has been rebranded to Cylance. **Note:** The preview period for enhanced authentication has ended and the updated sign-in flow is now the only method to access the Cylance console. Any authentication policies that you applied in your console during the preview period have taken effect.	June 2022

BlackBerry Connectivity Node version

- BlackBerry Connectivity Node version 2.12.1 (bundle 28.11.0). To download the latest version of the BlackBerry Connectivity Node, click here.

Management console and platform services fixed issues

Azure Active Directory Synchronization

You could not authenticate users synchronized from Azure Active Directory 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) displays devices that do not have the BlackBerry Protect Desktop agent installed. After a device has the BlackBerry Protect Desktop agent installed and is flagged as protected, the device is no longer displayed on the screen. If a user then uninstalls the BlackBerry Protect Desktop agent, the device is not displayed again on the unprotected devices screen. (UES-213)

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 2023)

Feature	Description
Script control setting for XLM macros in the device policy (Preview)	Administrators can now configure a script control setting in the device policy for protection against XLM macros. When a macro is executed, the agent responds to the Microsoft anti-malware scanning interface according to 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.

What's new in the management console for CylancePROTECT Desktop (November 2022)

Feature	Description
Auto-update Linux Driver	The CylancePROTECT Desktop agent 3.1.1000 for Linux devices can now request an update to the latest supported driver when an updated kernel is detected on the system. For example, if the Linux kernel is updated and the current installed 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 management console for CylancePROTECT Desktop (October 2022)

Feature	Description
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 date of the last scan for each device is logged in the management console. 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. You can also start the scan manually from the command line. This feature requires CylancePROTECT Desktop agent 3.1.1000 or later.

What's new in the management console for CylancePROTECT Desktop (March 2022)

Feature	Description
Exclusions for Dangerous VBA Macros	You can now add exclusions for the "Dangerous VBA Macro" violation type in the Memory Protection device policy. Any exclusion settings for macros in the Script Control device policy must be added to the Memory Protection device policy for devices running agent 3.0.1000. For more information about how to copy exclusions from Script Control to Memory Protection device policies, see KB 91485. For tenants managed from the Cylance multi-tenant console, see KB 92149.
Adding exclusions to Memory Protection device policies	When adding exclusions to a Memory Protection device policy, if you want the policy to apply to memory protection violations only and not script control violations, specify at least one violation type that you want to ignore. If you do not select any violation types to ignore, a warning message appears and the exclusion will apply to both Memory Protection and Script Control policies. For existing Memory Protection policies: • If the “Ignore Specific Violation Types” exclusion setting is already checked but the Script Control policy is not enabled, no action is required. • If the “Ignore Specific Violation Types” exclusion setting is unchecked and you want to ensure the policy is applied to memory protection violations only (and not script control), you must check it and specify at least one the violation type that you want to ignore.
Detection disabled for embedded VBScripts	Detection of embedded VBScript script control violations is disabled in CylancePROTECT Desktop agent 3.0.1000.
Memory Protection: Injection via APC	The “Injection via APC” violation type is now available in the Memory Protection device policy. You can also find these violations in the Exploit Attempts tab when viewing device details. For more information about using this violation type, see KB 92422.

Feature	Description
Memory Protection: Memory Permission Changes in Child Processes	The “Memory Permission Changes in Child Processes” violation type is now available in the Memory Protection device policy. You can also find these violations in the Exploit Attempts tab when viewing device details.
Renamed policy: Memory Permission Changes in Other Processes	The “Memory Permission Changes” memory protection violation type is now renamed to “Memory Permission Changes in Other Processes”.
Device Control: Read-only	For Windows devices running agent 3.0.1000, you can now allow read-only access to the following USB device types: • Still image • USB CD/DVD RW • USB drive • VMware USB passthrough • Windows portable device

What's new in the management console for CylancePROTECT Desktop (December 2021)

Feature	Description
Dangerous VBA macros	In a device policy, the macros feature has moved from Script Control to Memory Protection for devices running agent version 3.0.1000 or later. For agent versions 1584 and earlier, continue to use the macros feature under Script Control. For existing device policies, the policy will be updated the first time the policy is edited after this release. The policy update depends on the script control setting for macros. • If script control macros is disabled, then memory protection dangerous VBA macros is set to ignore. • If script control macros is set to alert, then memory protection dangerous VBA macros is set to alert. • If script control macros is set to block, then memory protection dangerous VBA macros is set to block. In the management console, the Memory Protection device policy UI states that this policy applies to agent version 1600, which is agent version 3.0.1000. For more information, see Script control in the Cylance Endpoint Security Setup content.

Feature	Description
Enhancements	• New exploitation, process injection, and escalation violation types have been added. When you edit the Memory Protection device policy, the settings for existing violation types are retained. By default, the new violation types are set to Ignore. • When you add an exclusion, a new "Ignore Specific Violation Types" check box displays on the Add Exclusion dialog box. If selected, you can then ignore the excluded file for any or all violation categories or individual violations under each category. When you add a memory protection exclusion, you must set at least one violation type to ignore. Otherwise, the exclusion is applied to memory protection and script control. • Injection by APC has been added as an exploitation violation type for memory protection. • On the Device Details page, operating system names were removed from some Memory Protection violation types. For example, the reference to Windows was removed from the "System DLL Overwrite" violation type. • Updates to memory protection events sent to Syslog servers are described in KB 70992.

What's new in the CylancePROTECT Desktop agent for Windows

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.

Feature	Description
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 date of the last scan for each device is logged in the management console. 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 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.

Feature	Description
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 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 2.1.1578

- Bug fixes only.
- The CylancePROTECT Desktop 1578 agent for Windows is supported on devices running Windows 11 and Windows Server 2022.

What's new in Windows agent version 2.1.1568

- Bug fixes only.

Note: The CylancePROTECT Desktop 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 3.1.1000

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 1580 agent did not properly log an action taken for the Remote APC Scheduled violation. (CHP-8534)

Fixed in Windows agent version 2.1.1578

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)
When "Watch For New Files" is enabled and a large number of files are copied to an excluded folder, the agent no longer causes high CPU usage and does not change status to offline. (EPP-1165)

Fixed in Windows agent version 2.1.1568

This release includes fixes that were released for agent version 2.1.1578.

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

On a device running Windows Server 2012 R2 and CylancePROTECT Desktop agent 3.1, `System32\wbem\WmiPrvSE.exe` is incorrectly reported as a threat. (EPP-3279)

Each time an executable that's in the exclusion list is run on a device, there are multiple redundant 'UNKNOWN_FILE' log entries associated with it. If the executable is used frequently, the log file size can grow quickly. (EPP-2828)

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.

If you plug in a UGREEN USB-C hub on a device that's running the CylancePROTECT Desktop agent with a device control policy, a blue screen error occurs. (EUS-934)

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.

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.

When adding a process exclusion to script control, `/[CySc_process]/` should automatically be added to the exclusion. When adding a process exclusion, make sure `//[CySc_process]/` is added to the exclusion list. If it is not added, manually add it to the process exclusion. (CCC-3727)

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)

In some Windows 10 environments, when attempting to upgrade to the 1580 agent, the automatic uninstallation of the previous agent might not be successful. (CHP-8288)

Workaround: Manually uninstall the previous agent and install the 1580 agent.

If the following conditions are met, 32-bit processes that do not have Program Control Flow Guard (CFG) enabled can stop responding:

- Windows Defender is enabled, and the System Control flow guard (CFG) setting is set to *on* under System Settings (Start menu > Windows Security > App & browser control > Exploit protection settings > System settings).
- CylancePROTECT agent 1580 is installed.
- Memory Protection is enabled.

(CHP-8262)

Workaround:

1. Go to **Start > Windows Security > App & browser control > Exploit protection settings > Program settings**.
2. Select the program that stopped responding and click **Edit**.
3. Scroll to Control Flow Guard (CFG) for the program and select the **Override system settings** checkbox.
4. Toggle the setting below the checkbox to **On**.
5. Click **Apply**.
6. Restart your computer.

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.

When the script control policy is enabled, launching the VisionApp Remote Desktop 2011 application results in an error. (MEM-830)

Workaround: Enable memory protection and add an exclusion for the VisionApp executable (for example, `C:\Program Files (x86)\visionapp Remote Desktop 2011\vRD70.exe`).

When script control is set to "Block" and memory protection is set to "Terminate" in a device policy, Microsoft OneNote 2016 does not successfully load. (MEM-779)

Workaround: In the script control settings for a device policy, allow the PowerShell console. Make sure the Block Powershell console usage feature is disabled.

For Windows 7 endpoints, if the memory protection policy is enabled and the "Remote Unmap of Memory process injection" setting is set to "Block", the parameters for the victim path and the image being unmapped are blank. This affects local and remote files. (MEM-747)

For known incompatibility issues with memory protection and script control with other products, see Known Memory Protection and Script Control Incompatibilities (KB 83016).

- This article helps users prepare before enabling memory protection or script control in their policies. For users who already have these features enabled and are not experiencing any issues, they are not affected by these incompatibilities.
- Cylance keeps track of these incompatibilities and attempts to resolve any issues whenever possible. The KB article includes a list of resolved issues and the related agent version

These conflicts are not unique to this release and do not solely depend on CylancePROTECT, as this may happen when any two applications monitor memory in the same way.

What's new in the CylancePROTECT Desktop agent for Linux

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 • Amazon Linux 2022 (Preview*) * Compatibility with the final released version of Amazon Linux 2022 will be confirmed upon its release.
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 date of the last scan for each device is logged in the management console. 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.

Feature	Description
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.

What's new in the Linux agent version 2.1.1590

Feature	Description
Added support for Linux distributions	Added support for the following Linux distributions: • RHEL/CentOS 7.9, 8.3 • Ubuntu 20.04 LTS • SUSE Linux 15 • Oracle 6, 7, 8 • Oracle UEK 6, 7, 8 • Debian 10 The Linux driver can be downloaded as a separate installation package. This allows users to update the Linux driver without waiting for a new release of the CylancePROTECT Desktop Linux agent. This release has the latest drivers, so installing the Linux driver package is not needed. If a new Linux driver becomes available before the next agent release, you can choose to upgrade the Linux driver at that time. If the Linux driver is updated manually, the zone-based updating feature in the console will not upgrade or downgrade the driver, unless a new major version is assigned. This is to prevent the automated system from overwriting an action taken by an administrator.

What's new in the Linux agent version 2.1.1580

Feature	Description
Added support for Linux distributions	Added support for the following Linux distributions: • RHEL/CentOS 7.9
Wildcards for memory protection exclusions	Memory protection exclusions now supports wildcards (*). For more information, see Use wildcards in Memory Protection exclusions.

Feature	Description
OS kernel reporting	The CylancePROTECT Desktop agent now reports OS kernel version of each device to the management console.
UEFI Secure Boot support	UEFI Secure Boot for Linux is now supported. To use this feature, you must use the CylancePROTECT Desktop Secure Boot CA certificate. For more information, see KB 73487.
Supported kernels spreadsheet	Additional Linux kernels are now supported. To view the full list of supported Linux kernels, download the Supported Linux Kernels spreadsheet.

Fixed issues in the Linux agent

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.

Fixed in Linux agent version 2.1.1590

There are no fixed issues in this release.

Fixed in Linux agent version 2.1.1580

A Blue Screen of Death (BSOD) error occurred on some systems when rebooting a HyperV host. (CHP-8221)
When memory protection was enabled on systems with other antivirus applications, it caused some applications to not launch. (CHP-8219, CHP-8243)
If the CylancePROTECT Desktop agent was configured to use a proxy, and the proxy service was stopped and the CylancePROTECT cloud services did not reconnect for some time, the agent used the local model instead. (CHP-8168)
In some environments if the ELF file had invalid section headers, the Cylance service repeatedly stopped and restarted. (CHP-8152)
A waived file was sending threat messages to Syslog each time the file ran. (CHP-8112)
The agent attempted to continuously upload a file to CylanceINFINITY. (CHP-8099)
If a signed file in a bundle was determined to be bad and was quarantined, the file was not removed from quarantine when the certificate was added to the global safelist. (CHP-7129)
The Self Protection option that was specified during agent installation couldn't be changed in the management console. (EPP-779)

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 3.1.1000.537

Item	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 date of the last scan for each device is logged in the management console. 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.

What's new for the macOS agent 3.0.1000.511

Item	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 2.1.1594.518

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 3.1.1000.537

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 3.0.1000.511

There are no fixed issues in this release.

Fixed issues in the macOS agent version 2.1.1594.518

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)

Fixed issues in the macOS agent version 2.1.1584.529

A macOS Big Sur system experienced performance degradation at startup when Memory Protection was enabled. (CHP-8375)
Fixed an issue with hash mismatches on a small set of files on a macOS operating system. (CHP-8306)

Known issues in the macOS agent

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

What's new in CylancePROTECT Mobile

Feature	Description	Date added
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
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
Update prompts for the CylancePROTECT Mobile app for Android	The CylancePROTECT Mobile app for Android version 2.3.0.1640 and later notifies the user when a new version of the app is available in Google Play. After 30 days, the CylancePROTECT Mobile app will download the update automatically and prompt the user to complete the update and restart the app. After 60 days, the user cannot use the app until they respond to the upgrade prompt.	April 2022

Feature	Description	Date added
Customize user notification methods	For each feature that you choose to enable in a CylancePROTECT Mobile policy, you can choose to notify users of threats using device notifications, email messages, or no notifications (users can view threat alerts in the CylancePROTECT Mobile app). For more information, see Create a CylancePROTECT Mobile policy.	April 2022
Localization of the CylancePROTECT Mobile app	The app is now available in French, German, and Japanese.	April 2022
Integration with Microsoft Intune to respond to mobile threats	The December release of the CylancePROTECT Mobile app adds support for integration with Microsoft Intune. The UI to configure integration with Intune will be added to the management console later in December 2021. You can connect Cylance Endpoint Security to Microsoft Intune to enable Cylance Endpoint Security to report a device risk level to Intune. The device risk level is calculated based on the detection of mobile threats by the CylancePROTECT Mobile app on Intune managed devices. Intune can execute mitigation actions based on the device risk level. For more information, see Integrating Cylance Endpoint Security with Intune to respond to mobile threats in the Cylance Endpoint Security Setup content.	Dec 2021

CylancePROTECT Mobile app versions

- CylancePROTECT Mobile app for iOS: 2.11.0.2954
- CylancePROTECT Mobile app for Android: 2.12.0.3252

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)

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)
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 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 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 (all platforms)

If a device is activated on BlackBerry UEM, internal apps that the user installs using the BlackBerry UEM Client are detected as sideloaded apps. (UESAPP-2125, UESAPP-2138, MTDLIB-165)

Workaround: Add the apps to the sideload detection safe list in the Cylance console.

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)

If you remove an app from the CylancePROTECT Mobile safe list or unsafe list, it can take up to 30 minutes for that change to take effect on devices (for example, if an app is removed from the safe list and is considered malicious by the CylancePROTECT cloud services, it can take up to 30 minutes for the CylancePROTECT Mobile app to detect it). If malware detection is turned off on in a CylancePROTECT Mobile policy and you turn it on, it can take up to 30 minutes for the CylancePROTECT Mobile app to start detecting malicious apps. (UESAPP-2547)

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 devices with iOS 16.2, if a user enabled SMS message filtering, the feature is turned off after the user upgrades the app. (UESAPP-3764) **Workaround:**: After upgrading the app, the user can turn SMS message filtering on again.
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

Note: With CylanceOPTICS version 3.0 and later, the CylanceOPTICS agent sends the device data that it collects to a centralized cloud architecture to be stored in a secure cloud database instead of storing the data locally on the device. This new architecture makes CylanceOPTICS cloud-enabled.

To manage this significant change for customers, BlackBerry is using the following approach to manage releases of the 3.x agent:

- For customers who have already contacted BlackBerry and have been granted the entitlement for CylanceOPTICS 3.x, the latest 3.x version of the agent is available in the management console.
- For customers who have CylanceOPTICS agent 2.x and do not have the entitlement for CylanceOPTICS 3.x, contact your BlackBerry Sales representative (or use the Contact Sales form) to request the latest 3.x agent and the entitlement for 3.x.

Agent version 2.5.x is still supported, but new features will require the latest 3.x agent. For more information about CylanceOPTICS agent 2.5.x, see the 2.5.x Administration Guide and Release Notes.

What's new in CylanceOPTICS (December 2022)

Feature	Description
New OS support	This release adds support for the following operating systems: • Windows 11 22H2 • Windows 10 22H2 • macOS Ventura (13.x) • SUSE Enterprise Linux 15 SP4 • Oracle Linux Server 7 (non-UEK) • Debian 11 • Debian 10 For more information about supported operating systems, see the Cylance Endpoint Security compatibility matrix. For more information about OS requirements, see CylanceOPTICS requirements in the Cylance Endpoint Security Setup content.

Feature	Description
CylanceOPTICS agent versions	• Windows: 3.2.1299.0 • macOS: 3.2.1299.5000 • Linux RHEL/CentOS 8: 3.2.1299-23000 • Linux RHEL/CentOS 7: 3.2.1299-7000 • Amazon Linux 2: 3.2.1299-15000 • Linux SLES15: 3.2.1299-29000 • Linux SLES12: 3.2.1299-21000 • Ubuntu 20.04: 3.2.1299-25000 • Ubuntu 18.04: 3.2.1299-17000 • Oracle Linux Server 8 / UEK 8: 3.2.1299-37000 • Oracle Linux Server 7: 3.2.1299-35000 • Debian 11: 3.2.1299-49000 • Debian 10: 3.2.1299-47000 For more information about supported operating systems, see the Cylance Endpoint Security compatibility matrix. For more information about OS requirements, see CylanceOPTICS requirements in the Cylance Endpoint Security Setup content.
MSI installer	This release introduces a new MSI installer package that you can use to install the CylanceOPTICS agent version 3.2 on Windows devices. For more information about the OS commands supported by the MSI installer, see OS commands for the CylanceOPTICS agent in the Cylance Endpoint Security Setup content.

What's new in CylanceOPTICS (October 2022)

Feature	Description
CylanceOPTICS agent versions	• Windows: 3.2.1140.0 • macOS: 3.2.1140.5000 • Linux RHEL/CentOS 8: 3.2.1140-23000 • Linux RHEL/CentOS 7: 3.2.1140-7000 • Amazon Linux 2: 3.2.1140-15000 • Linux SLES15: 3.2.1140-29000 • Linux SLES12: 3.2.1140-21000 • Ubuntu 20.04: 3.2.1140-25000 • Ubuntu 18.04: 3.2.1140-17000 • Oracle Linux Server 8 / UEK 8: 3.2.1140-37000 For more information about supported operating systems, see the Cylance Endpoint Security compatibility matrix. For more information about OS requirements, see CylanceOPTICS requirements in the Cylance Endpoint Security Setup content.

Feature	Description
Customized partial lockdown	CylanceOPTICS version 3.1 introduced the partial lockdown feature for Windows devices. This release introduces the ability to create custom partial lockdown configurations that allow you to specify additional communication channels that you want to allow during a partial lockdown. For more information, see Lock a device in the Cylance Endpoint Security Administration content.
Additional CylanceOPTICS administrator permissions	The July 2022 update of CylanceOPTICS introduced new administrator permissions that you could assign to roles to control how administrators engage with CylanceOPTICS. This release introduces additional CylanceOPTICS permission groups and sub-permissions, offering a greater level of access control and customization. If you previously granted an administrator role a CylanceOPTICS permission that was introduced in the July 2022 update, that role will be granted any associated sub-permissions that are introduced in this update. It is a best practice to review the CylanceOPTICS permissions that are introduced in this update so that you can make any adjustments that are appropriate for your organization's environment. For more information, see Permissions for administrator roles in the Cylance Endpoint Security Setup content.
Syslog messages for the API sensor	The late October update of the CylanceOPTICS cloud services will add a new event type that can be reported to SIEM solutions and syslog servers, OpticsCaeApiEvent. This event type is used for events that are detected by the CylanceOPTICS agent's optional API sensor. For more information about the API sensor, see CylanceOPTICS sensors in the Cylance Endpoint Security Setup content. For more information this new event type, see the Cylance Syslog Guide.
New audit log values for device lockdown syslog messages	The mid-October 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 feature: • DeviceUnlock • DeviceChangeLockdownProfile For more information about audit log events, see the Cylance Syslog Guide.

What's new in CylanceOPTICS (July 2022)

Feature	Description
New CylanceOPTICS administrator permissions	This update of the management console introduces new administrator permissions that you can configure and assign to administrator roles (Settings > Administrators > Roles), offering more granular access and management options for CylanceOPTICS features. Threat Protection > View, create, edit, delete CylanceOPTICS has been removed and replaced with a new Endpoint Detection Response section and new options under Users and Devices > View devices. If you previously created custom roles with the Threat Protection > View, create, edit, delete CylanceOPTICS permission enabled, those custom roles will have the new CylanceOPTICS permissions enabled when this update is applied to your environment. For more information, see Permissions for administrator roles in the Cylance Endpoint Security Setup content.
Navigation changes in the Cylance console	Changes have been made to the CylanceOPTICS menu navigation to make the experience consistent with other sections of the console and to make the CylanceOPTICS screens easier to access.
Enhancements to CylanceOPTICS syslog messages	The early August update of the CylanceOPTICS cloud services adds new fields to the CylanceOPTICS event types that can be reported to SIEM and syslog servers. The new fields are compatible with CylanceOPTICS agent 2.5.3000/3010 and agent 3.0 and later. For more information about the new fields, including example messages for each event type, see the Cylance Syslog Guide. New fields added to every CylanceOPTICS event type (process, file, registry, WMI, network, PowerShell, DNS, memory, log): • Event Timestamp • Event Received Timestamp • Device Last Reported Users • Zone Ids • Detection Rule Id • Instigating Process Command Line • Instigating Process File Path New fields added to process events: • Target Process Command Line • Target Process File Path New fields added to network events: • Source IP • Source Port Note that some fields will include command line values that can include commas and colons. BlackBerry recommends that you review and test the parsing of these values by your SIEM or syslog server.

Considerations when upgrading to 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 3.2

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 a whitelisted port value and you assigned it to a CylanceOPTICS device, the whitelisted port for partial lockdown was not removed when you assigned a different custom configuration. As a result, any ports that you whitelisted with any partial lockdown configuration remained whitelisted 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.
If the API Sensor is enabled in the device policy that is 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 may stop working. This issue is resolved in the next release of the CylanceOPTICS agent. (EDR-10871) **Workaround:** Turn off the API Sensor in the device policy.
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 run an advanced query and try to generate focus data from the results, the focus description that is used to generate the data does not include the correct artifact information. (EDR-9414)
If you downgrade from CylanceOPTICS agent version 3.1 or later to version 3.0, the lockdown feature stops working. (EDR-9199) **Workaround:** Uninstall agent version 3.0 and install it again.
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)
If a remote session is active when the CylanceOPTICS agent is installed on a macOS Big Sur (11.x) device, the session disconnects when the installation is complete. (EDR-7180) **Workaround:** Start the remote session again.
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)
When you view the results of an InstaQuery, the count for devices queried and devices responded might not be accurate. This issue occurs intermittently. (EDR-6523)
Performance counters for macOS and Linux do not include system counter data, such as CPU and memory. (EDR-5219)
If you use an ssh session to perform a silent uninstall of the CylanceOPTICS agent on a macOS Big Sur (11.x) device, /Applications/Cylance/ Optics/CyOpticsESFLoader.app remains and the system extension is still active. This issue occurs because Apple has no mechanism to silently uninstall system extensions without explicit confirmation by the end user. To resolve, use the finder to locate CyOpticsESFLoader.app and drag it to the trashcan, then confirm the UI prompt to deactivate and remove the system extension. For more information, see Troubleshooting: Removing the CylanceOPTICS agent from a macOS device.

CylanceGATEWAY release notes

What's new in the management console

Feature	Description	Date added
Network anomaly detection	CylanceGATEWAY uses machine learning to learn and monitor a CylanceGATEWAY user's upload volume and download behavior pattern. Network anomaly events are detected when a user's upload and download volume are not consistent with past behavior. Abnormal upload and download volumes could be an early indicator of compromise (for example, exfiltration attempts, or malicious software installed on the device). When an anomaly is detected, it is displayed on the CylanceGATEWAY Events screen and identified as a behavioral risk anomaly. This detection allows administrators to review the activity and determine if it is expected behavior. Behavioral risk anomalies do not block user traffic.	Jan 2023
Benign Domain Classification	CylanceGATEWAY uses machine learning that applies categorization to previously uncategorized destinations. This feature allows administrators to ensure compliance with their organization's acceptable use and regulatory requirements.	Dec 2022
C2 beacon detection	Beaconing is one of the first network-related indications of a botnet or a peer-to-peer malware infection. When a host is infected, the malware can initiate a command and control (C2) channel with its creator. CylanceGATEWAY now detects and reports beacons in your private network traffic. Identified C2 beacon events are labelled as Zero Day Detection and categorized as a security risk and subcategorized as a beacon. The anomaly detection threat events are sent to the SIEM solution or syslog server, if configured.	Dec 2022

Feature	Description	Date added
CylanceGATEWAY Events enhancements	On the CylanceGATEWAY Events page, • **Time is displayed in UTC format**: All timestamps (for example, Start Time and Event Details) are now displayed in UTC format. This feature allows for easy correlation with other security products that use UTC format for time. This feature also allows administrators to filter events for a specific time without having to consider users that might be in different time zones. • **Event Details page**: The link to view a summary of a user's network activity has been moved from the Events page to the Event Details page. • **Control the order of the columns**: You can now change the order of the events columns by dragging the column to where you want it to appear. The updated order of the columns is saved in the local browser that you used to view the page. This feature allows administrators to order the events columns to their preference. • **UI update**: The Connector column has been replaced with the Network Route column. The Network Route column will label traffic as Public or Private. For Private connections, the CylanceGATEWAY Connector that is used to route the traffic will be identified. The Network Route column can be filtered to display Public traffic, Private traffic, or traffic for a specified CylanceGATEWAY Connector. • **Filter capabilities**. You can now perform free form type to search the events. As you type characters in the search field, you can select from the displayed matching options. The enhanced filter capability provides you with an alternate method to filter the events. • **Network events deep linking**: You can copy a link to an event using the icon added to the top of the event details page and share it with another console user to view the specific filtered event. This feature allows administrators to facilitate multi-team collaboration during an audit or investigation of destinations that users have tried to access. Console users must have the appropriate permissions to view the event. • **New user search capabilities**: You can now filter events by users' Active Directory username from the user filter in events. Select the filter option and type the user's Active Directory username in the search field. This filter allows administrators and SOC analysts to investigate events for a specific user and allows for better correlation between CylanceGATEWAY and other security tools.	Dec 2022
Gateway Connectors info enhancements	The Connection History Time is now displayed in UTC format. This feature allows administrators to view the latest status of a CylanceGATEWAY Connector without having to consider if the connector was installed in a different time zone.	Dec 2022

Feature	Description	Date added
Google Workspace as Managed Service	Administrators can now easily configure access to the Google Workspace set of applications such as Gmail, Google Drive, and Google IM & VoIP without having to know their FQDNs or IP addresses. This feature simplifies the process of configuring access to these destinations in the ACL rules.	Dec 2022
iOS and Android device posture validation on connect	Administrators can require iOS and Android devices to be managed by Microsoft Intune before users can use CylanceGATEWAY. For more information, see Configure CylanceGATEWAY service options in the Cylance Endpoint Security Setup content.	Sept 2022

CylanceGATEWAY component versions

- CylanceGATEWAY Connector version 2.7.0.775
- CylanceGATEWAY agent for Windows version 2.5.0.5
- CylanceGATEWAY agent for macOS version 2.5.16

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

What's new in CylanceGATEWAY Connector 2.7.0.775 (Dec 2022)

Feature	Description
Amazon Web Services (AWS) deployment support	The CylanceGATEWAY Connector can now be deployed in an AWS Cloud environment. This feature allows CylanceGATEWAY users to access resources in their private network when the private network is hosted in the AWS Cloud through the CylanceGATEWAY Connector.

CylanceGATEWAY fixed issues

Fixed issues in the CylanceGATEWAY agent for macOS

Fixed issues in the CylanceGATEWAY agent for macOS 2.5.16 (Aug 2022)

Changes to the local CylancePROTECT Serial Number on macOS devices, when not propagated to the management console by the CylanceGATEWAY client, may have resulted in a failure to activate or enable Work Mode on macOS CylanceGATEWAY endpoints. (BIG-8030)

Fixed issues in the CylanceGATEWAY agent for macOS 2.0.17 (May 2022)

When some users that ran the CylancePROTECT agent on macOS devices tried to enable work mode, the client remained at 'enabling work mode' and didn't enable. (BIG-6935)

CylanceGATEWAY known issues

Access control list (ACL)

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

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).

Device

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
```

Agent

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

CylanceAVERT release notes

What's new in the management console

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 File Inventory in the BlackBerry Avert Administration and Overview 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 Evidence locker in the BlackBerry Avert Administration and Overview guide for more information.

CylanceAVERT fixed issues

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.
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 Azure 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