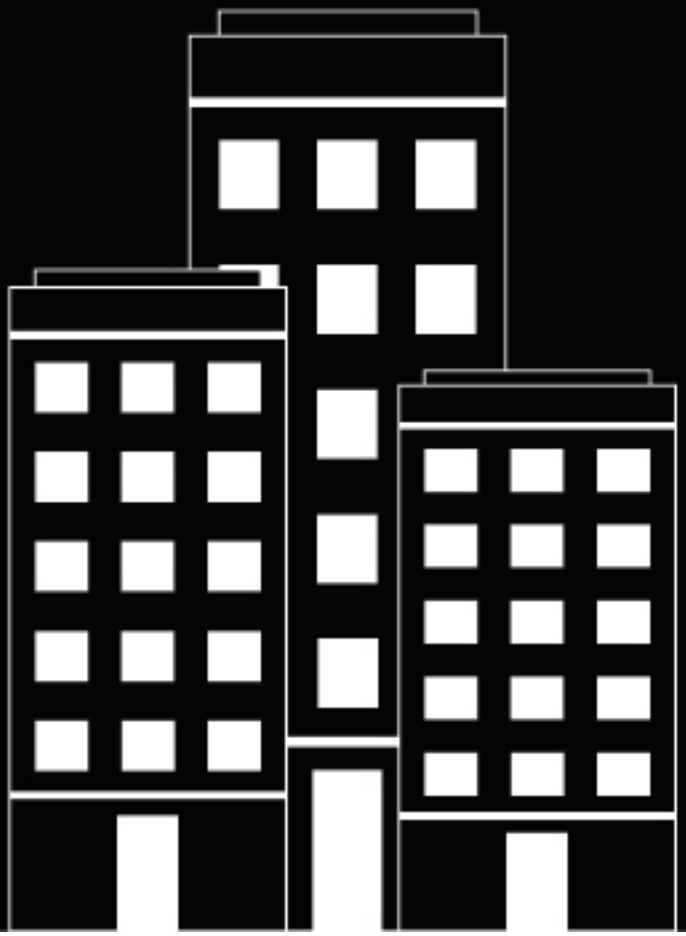
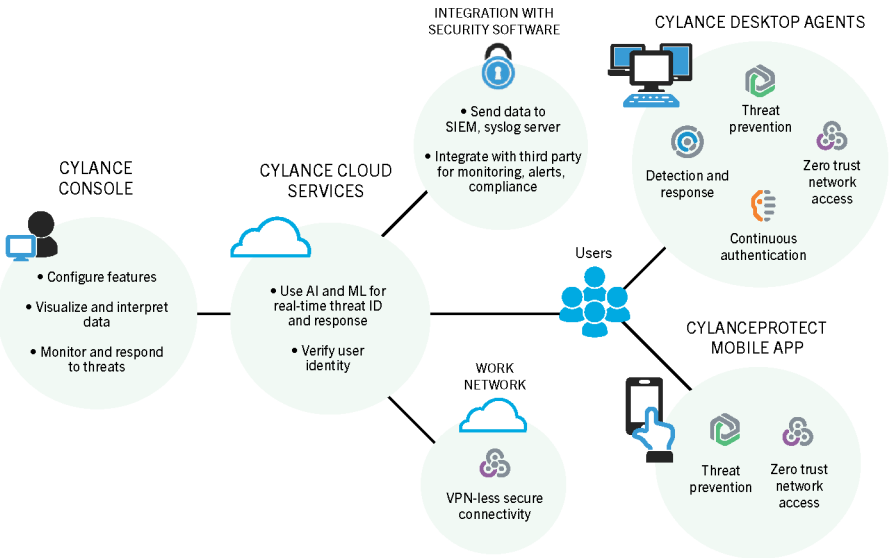


Cylance Endpoint Security

Overview and Architecture Guide

Contents

What is Cylance Endpoint Security?



Cylance Endpoint Security provides a unified endpoint security solution that is designed for the new reality. It consolidates the best available AI-driven tools to detect, protect against, and remediate threats on every endpoint. Today's cyber criminals use artificial intelligence (AI) to create increasingly advanced threats that maximize the reach and impact of their attacks. Today's solutions must also take advantage of the power of machine learning and AI. Cylance Endpoint Security provides an AI-powered solution for Zero Trust across the spectrum of devices, networks, apps, and people.

The Zero Trust approach modernizes network security while simultaneously enhancing and improving the network experience for end users. The Zero Trust security model trusts nothing and no one by default, including users inside the work network. Every user, endpoint, and network is assumed to be potentially hostile. In Zero Trust security, no user can access anything until they prove who they are, that their access is authorized, that the network they are connected to is not compromised, and that they, or malware hiding on their device, are not acting maliciously.

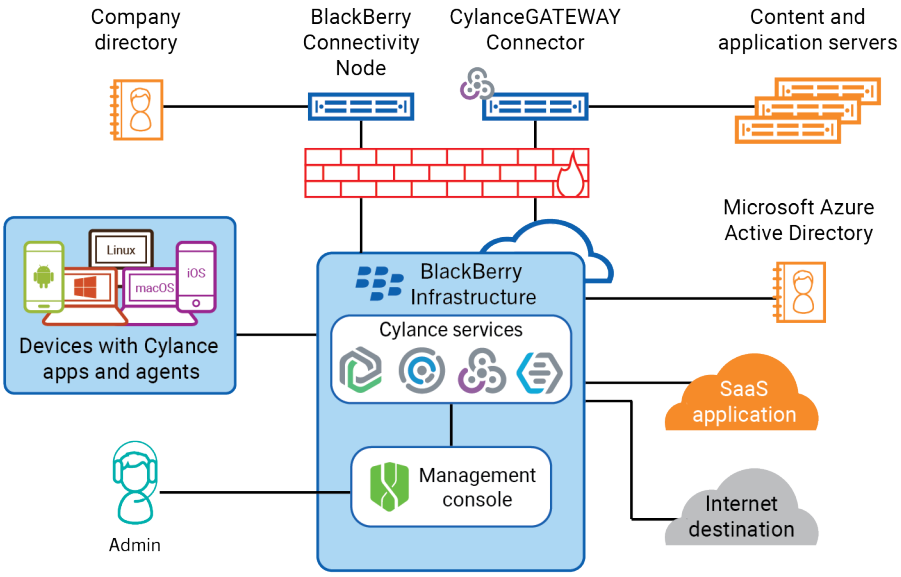
Key features of Cylance Endpoint Security

Cylance Endpoint Security offers a broad set of security capabilities through several interconnected features:

Feature	Description
Detect and block ransomware, malware, and other threats	CylancePROTECT Desktop blocks ransomware and other malware on Windows, macOS, and Linux devices using a mathematical approach to malware identification. It uses machine learning techniques instead of reactive signatures, trust-based systems, or sandboxes to provide endpoint detection and response that renders new ransomware, malware, viruses, bots, and future variants useless. CylancePROTECT Desktop analyzes potential file executions for ransomware and other malware in the OS and memory layers to prevent the delivery of malicious payloads.

Feature	Description
Mobile device protection	CylancePROTECT Mobile provides mobile threat defense for iOS, Android, and Chrome OS devices. In addition to malware identification, CylancePROTECT Mobile also detects sideloaded apps, malicious URLs in text messages, and other security risks, and recommends specific actions to eliminate the threat.
Attack detection and response	CylanceOPTICS monitors your Windows, macOS, and Linux devices and lets you know when your organization may be under attack. CylanceOPTICS collects information from devices and aggregates it using cloud services to track, alert upon, and respond to malicious events as soon as they occur. CylanceOPTICS can stop attacks before they execute and automate investigation and response to attacks.
Secure access to your network and your cloud-based services	CylanceGATEWAY provides Zero Trust Network Access (ZTNA) for your users' iOS, Android, Windows, and macOS devices to secure user access to your extended network perimeter and protect your extended network from threats. CylanceGATEWAY protects devices by allowing you to block connections to Internet destinations that you don't want devices to reach, even when the device isn't connected to your network. CylanceGATEWAY protects your private network and cloud-based services by allowing access only to authorized users.
Sensitive data protection	CylanceAVERT identifies and categorizes sensitive data on Windows devices in your organization's environment to create a sensitive file inventory and notify specified users when sensitive data is involved in an exfiltration event. CylanceAVERT can scan files that are copied to a USB device, uploaded to a browser location or network drive, or in the body content or the attachments of email messages, and recommend a remediation action.
Work with any UEM or MDM platform	Cylance Endpoint Security can be used with BlackBerry UEM to provide the highest level of endpoint management and security to protect your organization against a wide array of threats. If you have an Unified Endpoint Management (UEM) or Mobile Device Management (MDM) platform other than BlackBerry UEM, you can use Cylance Endpoint Security to better protect your endpoints and the data travelling between them and your network. Over time, specific integrations with MDM solutions like UEM and Microsoft Intune will be added to Cylance Endpoint Security to enhance your ability to manage devices in response to potential threats.

Cylance Endpoint Security architecture



Component	Description
BlackBerry Infrastructure	The BlackBerry Infrastructure is a global private data network distributed across multiple regions that enables and secures data in transit between thousands of organizations and millions of users around the world. It is designed to efficiently manage the transport of data between BlackBerry services and end-user devices. The BlackBerry Infrastructure registers user information for agent and CylancePROTECT Mobile app activation, validates licensing information, and maintains a trusted connection with on-premises components installed behind the firewall and with agents and the CylancePROTECT Mobile app on users' devices inside and outside the firewall.
CylancePROTECT	CylancePROTECT Desktop detects and blocks malware on Windows, macOS, and Linux devices using machine learning techniques to render new malware, viruses, bots, and future variants useless. CylancePROTECT Mobile detects malware, sideloaded apps, malicious URLs in text messages, and other security risks on iOS, Android, and Chrome OS devices, and recommends action to eliminate the threat.
CylanceOPTICS	CylanceOPTICS monitors Windows, macOS, and Linux devices and aggregates collected information to detect, track, alert upon, and respond to malicious events as soon as they occur. CylanceOPTICS can help you detect attacks when they start and automate investigation and response to stop them before they cause harm.
CylanceGATEWAY	CylanceGATEWAY protects network access for your organization's private network and cloud-based applications that both gives your Windows, macOS, iOS, and Android users access to your extended network perimeter and protects your extended network from threats.

Component	Description
CylanceAVERT	CylanceAVERT detects and prevents the loss of sensitive regulatory and organizational information through external sources. CylanceAVERT can discover, categorize, and inventory sensitive company information and provide threat detection to prevent unauthorized exfiltration events.
Cylance Endpoint Security cloud services	The Cylance Endpoint Security cloud services are the brain power behind each Cylance Endpoint Security feature. The cloud services for different features leverage AI, machine learning, or a risk engine based on user modeling to process large volumes of complex data to identify and respond to threats. For more information, see How Cylance Endpoint Security uses advanced technology to protect users and devices.
Management console	The cloud-based management console allows you to set up, manage, and monitor all of the features of Cylance Endpoint Security.
Devices with agents or the CylancePROTECT Mobile app	Agents installed on Windows, macOS, and Linux devices and the CylancePROTECT Mobile app installed on iOS, Android, and Chrome OS devices communicate with Cylance Endpoint Security to detect potential threats and take action to protect your users, devices, and network.
BlackBerry Connectivity Node	The BlackBerry Connectivity Node is an optional component that allows Cylance Endpoint Security to synchronize users and groups with your on-premises Microsoft Active Directory or LDAP directory. Cylance Endpoint Security can synchronize users and groups with Entra Active Directory without the BlackBerry Connectivity Node.
CylanceGATEWAY Connector	The CylanceGATEWAY Connector is an optional component that you can install behind your firewall and in private cloud networks to establish a secure tunnel between the BlackBerry Infrastructure and your private network. The CylanceGATEWAY Connector allows users to communicate with content and application servers behind your firewall using CylanceGATEWAY instead of a traditional VPN.

How Cylance Endpoint Security uses advanced technology to protect users and devices

CylancePROTECT Desktop and CylancePROTECT Mobile leverage cutting-edge cloud services to determine whether software, files, and websites are potentially malicious and a threat to the security of a device. The CylancePROTECT cloud services use sophisticated AI, machine learning, and efficient mathematical models to process large volumes of data from global sources, retain and continuously learn from the patterns and properties of that data, and use that data to make intelligent predictions and decisions about the risk potential of software, files, and Internet destinations in near-real time. The CylancePROTECT services constantly evolve to address new cyber threats, providing an aggressive and proactive security strategy that identifies malicious software and websites before they can have any impact on your organization's infrastructure or device users.

The CylancePROTECT services provide the threat analysis for files that are scanned by the CylancePROTECT Desktop agent. If a file is identified as malicious, the CylancePROTECT Desktop agent will perform any mitigation actions that you configured (for example, alert or quarantine). The agent includes a local CylancePROTECT

service model, so if the agent cannot communicate with the cloud, the agent will use the local model to score a file.

CylanceGATEWAY provides machine learning models (for example, Signature detection and DNS Tunneling detections) and continuous monitoring and dynamic application of IP reputation databases to monitor network traffic and identify destinations that might contain potentially malicious threats. If a destination is identified as containing potential threats, CylanceGATEWAY will perform any the actions that you have configured (for example, alert or block the connection to the destinations). CylanceGATEWAY provides two modes of operation, Work Mode and Safe Mode, to protect users' devices and your network from threats.

The CylancePROTECT services are a core component of several CylancePROTECT Mobile features, including malware detection, SMS message scanning, and secure network checks. If CylanceGATEWAY is enabled, the CylancePROTECT Mobile app also uses machine learning to continuously monitor network traffic and can block a user’s access to a destination.

The CylanceOPTICS agent on desktop devices sends the data that it collects to the CylanceOPTICS cloud services. The data is aggregated and stored in the secure CylanceOPTICS cloud database. The CylanceOPTICS data analytics services offer rich interpretations of device data that you can access in the management console. CylanceOPTICS uses a Context Analysis Engine (CAE) to analyze and correlate events as they occur on devices. You can configure CylanceOPTICS to take automated response actions when the CAE identifies certain artifacts of interest (for example, display a notification or log off the current user), providing an additional layer of threat detection and prevention to complement the capabilities of CylancePROTECT Desktop.

The CylanceGATEWAY agent on desktop devices uses machine learning and static reputation databases to identify destinations that might contain potentially malicious threats. If the agent is also enabled for and using Safe Mode, CylanceGATEWAY will enforce an acceptable use policy (UAP) by intercepting each DNS query to determine if connection can proceed or is blocked.

The CylanceAVERT agent identifies the sensitive files on an endpoint and notifies the administrator of any attempt to exfiltrate those files through email, browser uploads, network drives, or USB devices. If a sensitive file is involved in an exfiltration event, CylanceAVERT will perform the mitigation action that the administrator specified in the information protection settings. CylanceAVERT uses keyword matching and regex validation to identify the sensitive data types that trigger an exfiltration event.

What is CylancePROTECT Desktop?

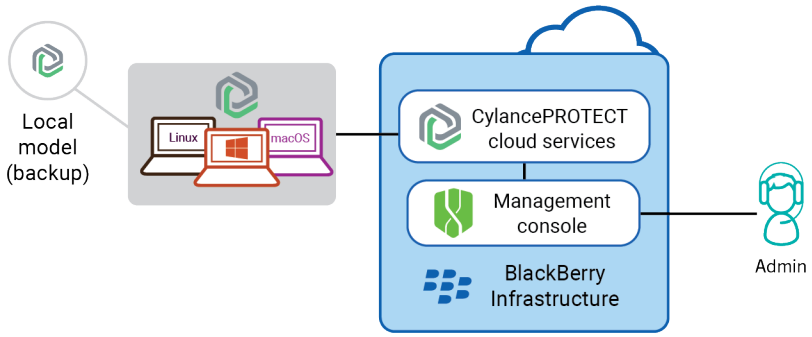
CylancePROTECT Desktop detects and blocks malware before it can affect a device. BlackBerry uses a mathematical approach to malware identification, using machine learning techniques instead of reactive signatures, trust-based systems, or sandboxes. This approach renders new malware, viruses, bots, and future variants useless. CylancePROTECT Desktop analyzes potential file executions for malware in the OS and memory layers to prevent the delivery of malicious payloads.

The CylancePROTECT Desktop agent is designed to use a minimal amount of system resources. The agent treats files or processes that execute as a priority because these events could be malicious. Files that are simply on disk (in storage but not executing) take a lower priority because while these could be malicious, these do not pose an immediate threat.

Key features of CylancePROTECT Desktop

Feature	Description
Detect and quarantine malicious files	CylancePROTECT Desktop provides options for handling files that it detects as either unsafe or abnormal. You can add files identified in threat events to a quarantine list or a safe list for handling future events.
Protect against memory exploits	CylancePROTECT Desktop provides options for handling memory exploits, including process injections and escalations. You can also add executable files to an exclusion list, allowing these files to run when a device policy is applied.
Block malicious scripts	CylancePROTECT Desktop monitors and protects against malicious scripts running in your environment. The CylancePROTECT Desktop agent is able to detect the script and script path before the script is executed and block it.
Block threats from USB storage devices	CylancePROTECT Desktop controls how USB mass storage devices can connect to devices in your organization. You can allow or block USB mass storage devices, including USB flash drives, external hard drives, and smartphones.
Receive immediate alerts	CylancePROTECT Desktop monitors the execution of malicious processes and alerts you when anything unsafe or abnormal attempts to run.
Detect inactive devices	If the CylancePROTECT Desktop agent has been out of contact for a specified period of time, the device state changes to inactive. You can review inactive devices to determine if they should be removed from the management console.
Protect virtual machines	CylancePROTECT Desktop is not as resource intensive on a per-guest basis because the technology does not require daily disk scans. CylancePROTECT Desktop is also not as memory intensive on a per-guest basis.

Architecture: CylancePROTECT Desktop



Item	Description
CylancePROTECT cloud services	CylancePROTECT Desktop detects and blocks malware using machine learning techniques to render new malware, viruses, bots, and future variants useless. The CylancePROTECT cloud services use sophisticated AI, machine learning, and efficient mathematical models to process large volumes of data from global sources, retain and continuously learn from the patterns and properties of that data, and use that data to make intelligent predictions and decisions about the risk potential of software, files, and Internet destinations in near-real time. The CylancePROTECT services provide the threat scoring for files that are scanned by the CylancePROTECT Desktop agent. The file score determines what action the agent should take for the file, based on the device policy assigned to the agent.
Management console	The cloud-based management console allows you to view various threat-related events, manage device policies to configure agents on endpoints, and manage global lists for quarantined and safe files.
Devices with the CylancePROTECT Desktop agent	The CylancePROTECT Desktop agent must be installed on a device (endpoint) to protect the device. CylancePROTECT Desktop supports Windows, macOS, and Linux operating systems.
Local model	The CylancePROTECT Desktop agent on each endpoint maintains a secondary copy of the model that the CylancePROTECT services use to score files. If the agent is unable to connect to the CylancePROTECT services, the local model calculates file scores.

What is CylancePROTECT Mobile?

CylancePROTECT Mobile is an advanced security solution that proactively identifies and prevents cyber threats on iOS, Android, and Chrome OS devices in real time without disrupting the productivity of your workforce.

CylancePROTECT Mobile uses a combination of leading-edge technologies, including:

- The web-based management console that you use to manage mobile devices, manage CylancePROTECT Mobile features, and view details about mobile threats
- The CylancePROTECT Mobile app that scans a user's device in regular intervals to detect threats and give an overall security assessment. Whenever possible, the app gives the user clear direction to resolve threats without administrator intervention
- The CylancePROTECT cloud services that use sophisticated AI and machine learning to support key CylancePROTECT Mobile features, including the real-time identification of malware and unsafe URLs in text messages

The seamless integration of these technologies establishes a secure ecosystem where data is protected and malicious activities are identified on mobile devices and eliminated proactively. CylancePROTECT Mobile is easy to configure, easy for end users to understand and use, and leverages cloud technologies that are always improving and getting smarter.

Key features of CylancePROTECT Mobile

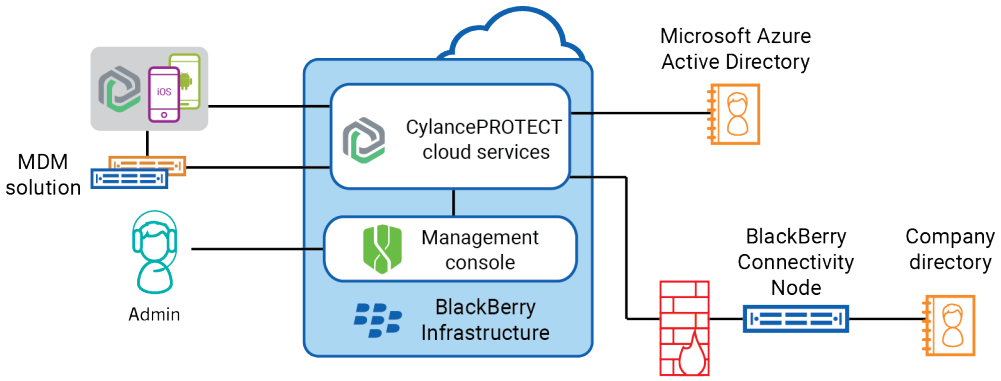
Feature	Description
Malware detection for Android devices	The CylancePROTECT Mobile app can detect malware on an Android device and direct the user to uninstall malicious apps. The CylancePROTECT Mobile app scans the apps on a user's device and uploads the app files to the CylancePROTECT cloud services, which use AI and machine learning to analyze the app package and produce a confidence score that it returns to the CylancePROTECT Mobile app. The confidence score determines whether the scanned app is safe or potentially malicious. When the CylancePROTECT services determine that an app is potentially malicious, the app notifies the user and provides further details. The user can tap a fix option in the app to navigate to the device settings and uninstall the malicious app. An app is uploaded to the CylancePROTECT services if it has a hash that the services have not processed previously. If the device scan finds an app that has been analyzed previously, it uses the confidence score that the CylancePROTECT services have already generated for that unique app hash. Whenever an app has a new hash (for example, for a new version) the app is uploaded to the CylancePROTECT services for analysis and scoring (if it has not already been uploaded from another device).

Feature	Description
Sideload detection for iOS and Android devices	Sideloaded apps don't follow the same restrictions or protections as apps distributed through official app stores. The CylancePROTECT Mobile app can detect the presence of a sideloaded app on a user's device, alert the user, and guide the user to uninstall it. On iOS, the CylancePROTECT Mobile app can detect only sideloaded app developer certificates that the user has chosen to trust in the device settings. A user can't use a sideloaded app unless the app developer certificate has been trusted. On Android, the CylancePROTECT Mobile app identifies sideloaded apps based on the installation source. The CylancePROTECT cloud services and the CylancePROTECT Mobile app consider official app sources, such as Google Play, the Amazon Appstore, and the Samsung Galaxy Store, to be trusted. Apps that were installed from untrusted sources are considered sideloaded. **Note:** Sideload detection is not supported for iOS 17.5 and later.
Scanning URLs in SMS text messages on iOS devices	CylancePROTECT Mobile can warn users of potentially malicious URLs in SMS text messages. New incoming text messages from known contacts are automatically considered to be safe and only messages from unknown senders are scanned and assessed. When a user receives an SMS text message that contains a URL, the CylancePROTECT Mobile app sends the entire message to the CylancePROTECT cloud services in real time. The CylancePROTECT services use advanced machine-learning capabilities and accumulated knowledge from threat intelligence feeds to provide an instant assessment of the safety of the message. When an unsafe URL in a text message is detected, the message is filtered to the junk folder. To protect user privacy, only messages that contain URLs are assessed. No additional metadata or user identifiers are collected or stored.
Scanning URLs in SMS text messages on Android devices	CylancePROTECT Mobile can warn users of potentially malicious URLs in SMS text messages. When a user receives an SMS text message that contains a URL, the unaltered URL is sent to the CylancePROTECT cloud services in real time. SMS scanning is limited to the default SMS app on the device. New incoming text messages from known contacts and unknown senders are scanned and assessed. The CylancePROTECT services use advanced machine-learning capabilities and accumulated knowledge from threat intelligence feeds to provide an instant assessment of the safety of the URL. If a URL is determined to be unsafe, the CylancePROTECT Mobile app alerts the user, provides details, and guides the user to delete the text message. To protect user privacy, only messages that contain URLs are assessed. No additional metadata or user identifiers are collected or stored.

Feature	Description
Unsafe network and insecure Wi-Fi checks	CylancePROTECT Mobile defends against the following network threats: • Unsafe network connections: On iOS and Android devices, the CylancePROTECT Mobile app will periodically try to connect to the CylancePROTECT cloud services. If the connection is not successful, CylancePROTECT Mobile determines that the network is not safe. • Insecure Wi-Fi access points: On Android devices, the CylancePROTECT Mobile app periodically checks the properties of the current Wi-Fi access point to determine if it is secure. You can configure which Wi-Fi access algorithms your organization considers secure and insecure. When the CylancePROTECT Mobile app detects an unsafe network or insecure Wi-Fi access point, it is reported in the app and in the management console.
Device security checks	The CylancePROTECT Mobile app checks specific device conditions and security settings and notifies the user about potential vulnerabilities to cyber threats. The app checks the following: • Whether developer mode is enabled (Android only) • Whether disk encryption is enabled (Android only) • Whether a screen lock is enabled (for example, a password or fingerprint) • Whether the device is rooted or jailbroken • Whether the device is running an OS version that you do not want to support • Whether the device model is one that you do not want to support If the app detects a vulnerability, it indicates the potential risk level and provides guidance for the user to resolve the issue.
Attestation checks	The CylancePROTECT cloud services can regularly perform attestation checks to verify the integrity and security of the CylancePROTECT Mobile app on each user's device. On Android devices, the CylancePROTECT cloud services use Play Integrity attestation, SafetyNet attestation, and hardware certificate attestation to validate the CylancePROTECT Mobile app. Play Integrity attestation replaces SafetyNet attestation. Older versions of the app will continue to support SafetyNet attestation until Google removes support. Attestation checks occur daily. You can also enforce a minimum security patch level on devices. If the app detects that the device does not meet the required patch level, it can alert the user to check for updates. On iOS devices, the CylancePROTECT cloud services check the integrity of the app using the Apple DeviceCheck framework. Integrity checks occur daily. On Samsung devices, the CylancePROTECT cloud services can also use Samsung Knox Enhanced Attestation in regular intervals to validate the integrity of devices. Knox Enhanced Attestation is hardware-based and can detect device tampering, rooting, OEM unlock, and IMEI or serial number falsification, in addition to performing app health checks. If an attestation failure occurs, administrators can view details in the management console.

Feature	Description
Integration with MDM solutions	You can connect Cylance Endpoint Security to Microsoft Intune so that Cylance Endpoint Security can report a device risk level to Intune. The device risk level is calculated based on the detection of mobile threats by the CylancePROTECT Mobile app on Intune managed devices. Intune can execute mitigation actions based on the device risk level.
Usability features of the CylancePROTECT Mobile app	For each feature that you choose to enable in the CylancePROTECT Mobile app, you can choose to notify users of threats using device notifications, email messages, or no notifications (users can view threat alerts in the CylancePROTECT Mobile app). The CylancePROTECT Mobile app for Android version 2.3.0.1640 and later notifies the user when a new version of the app is available in Google Play. After 30 days, the app will download the update automatically and prompt the user to complete the update and restart the app. After 60 days, the user cannot use the app until they respond to the upgrade prompt. The CylancePROTECT Mobile app for iOS supports automatic updates from the App Store.

Architecture: CylancePROTECT Mobile



Item	Description
CylancePROTECT cloud services	The management console and the CylancePROTECT Mobile app on users' devices use a secure connection to communicate with the CylancePROTECT cloud services, which are responsible for creating and configuring user accounts, applying CylancePROTECT Mobile features and settings to devices, and processing events and alerts in real time. The CylancePROTECT services use AI and machine learning to determine whether software and websites are potentially malicious and a threat to the security of a device. This AI engine is a core component of several CylancePROTECT Mobile features, including malware detection, SMS message scanning, and network security validation. At its core, the AI engine enables an aggressive and proactive security strategy, identifying malicious software and websites before they can have any impact on your organization's infrastructure or device users.
Management console	The cloud-based management console allows you to manage mobile devices, configure and manage CylancePROTECT Mobile features, and view device status and the mobile alerts that are detected by the CylancePROTECT Mobile app.
BlackBerry Connectivity Node	The BlackBerry Connectivity Node is an optional component that allows Cylance Endpoint Security to synchronize CylancePROTECT Mobile users and groups with your on-premises Microsoft Active Directory or LDAP directory. Cylance Endpoint Security can synchronize users and groups with Entra Active Directory without the BlackBerry Connectivity Node.
Devices with the CylancePROTECT Mobile app	The CylancePROTECT Mobile app installed on iOS, Android, and Chrome OS devices scans the device in regular intervals and checks device settings and conditions to identify threats. When the app detects a threat, the user can view details in the app. Whenever possible, the app gives the user direction to resolve a threat and guides them to the device settings where they can address the issue.
MDM Solution	Optionally, you can connect Cylance Endpoint Security to Microsoft Intune so that Cylance Endpoint Security can report a device risk level to Microsoft Intune. The device risk level is calculated based on the detection of mobile threats by the CylancePROTECT Mobile app on Intune-managed devices. Intune can execute mitigation actions on devices based on the device risk level.

What is CylanceOPTICS?

CylanceOPTICS is an endpoint detection and response solution that collects and analyzes forensic data from devices to identify and resolve threats before they impact your organization's users and data.

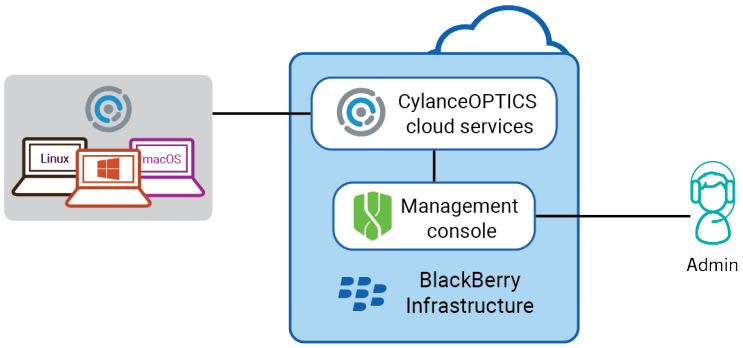
You enable a Windows, macOS, or Linux device for CylanceOPTICS by installing the CylanceOPTICS agent alongside the CylancePROTECT Desktop agent. The CylanceOPTICS agent deploys sensors into the OS at various levels and subsystems to monitor and collect a diverse set of data that is aggregated and stored in the CylanceOPTICS cloud database. You can use CylanceOPTICS data to detect, investigate, diagnose, and configure automated responses to device-based threats.

Key features of CylanceOPTICS

Feature	Description
Analyze CylanceOPTICS data	You can use the management console to query the device data collected by the CylanceOPTICS agent to investigate security incidents and discover indicators of compromise. When CylanceOPTICS identifies a file as a potential threat, you can retrieve the file from the device for further analysis. InstaQuery allows you to interrogate a set of devices about a specific type of forensic artifact, and allows you to determine whether an artifact exists on devices and how common that artifact is. Advanced query is an evolution of InstaQuery that provides more granular search capabilities using EQL syntax to enhance your ability to identify threats.
Visualize CylanceOPTICS data	You can use the following visualization features to assist your forensic analysis: • The InstaQuery facet breakdown provides an interactive visual display of the different facets involved in a query so that you can identify and follow their relational paths. • Focus data allows you to visualize and analyze the chain of events, and the associated artifacts and facets of those events, that resulted in a piece of malware or another security threat on a device.
Detect and respond to events	CylanceOPTICS uses the Context Analysis Engine (CAE) to analyze and correlate events as they occur on devices in near-real time. You can configure CylanceOPTICS to take automated response actions when the CAE identifies certain artifacts of interest (for example, display a notification or log off the current user), providing an additional layer of threat detection and prevention to complement the capabilities of CylancePROTECT Desktop. You can customize the detection capabilities of CylanceOPTICS to suit your organization's needs. You can create detection rule sets with your desired configuration of rules and responses, you can clone and modify existing detection rules or create your own custom rules, and you can create detection exceptions to exclude specific artifacts from detection.

Feature	Description
Deploy packages to collect data	You can use the package deploy feature to remotely and securely run a process (for example, a Python script) on CylanceOPTICS devices to collect and store desired data in a specified location for further analysis. For example, you can run a process to collect browser data. You can use the CylanceOPTICS data collection packages that are available in the management console or you can create your own.
Lock devices to isolate threats	You can lock an infected or potentially infected device, disabling its LAN and Wi-Fi network capabilities to stop command and control activity, the exfiltration of data, or the lateral movement of malware. Various lockdown options are available to suit your organization's needs.
Send actions to devices	You can use the remote response feature to securely execute scripts and run commands on any CylanceOPTICS-enabled device directly from the management console, using a familiar command line interface.

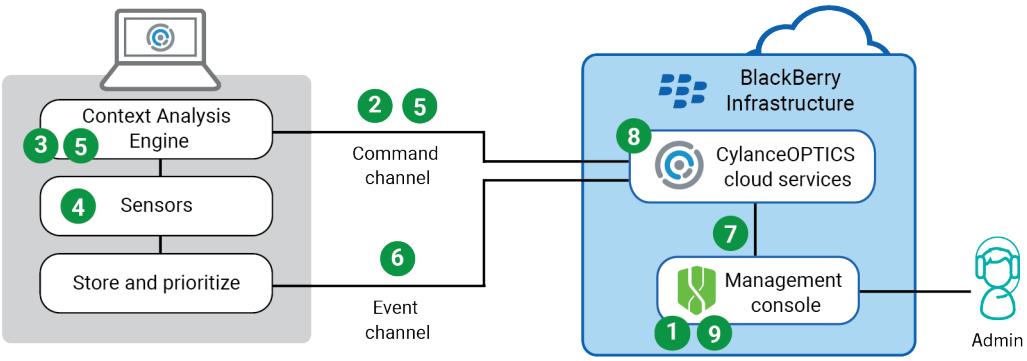
Architecture: CylanceOPTICS



Component	Description
CylanceOPTICS cloud services	The CylanceOPTICS agent sends the device data that it collects to the CylanceOPTICS cloud services. The data is aggregated and stored in the secure CylanceOPTICS cloud database. The CylanceOPTICS data analytics services offer rich interpretations of device data that you can access using the management console. For devices with the CylanceOPTICS agent version 2.x and earlier, the CylanceOPTICS database is stored locally on the device. Version 3.0 and later automatically aggregates, stores, compresses, and sends the data to the CylanceOPTICS cloud database at regular intervals.
Management console	The cloud-based management console allows you to manage CylanceOPTICS agents installed on devices, query CylanceOPTICS data to investigate security incidents, customize what CylanceOPTICS monitors and how it responds to events, and execute actions in response to threats.

Component	Description
Devices with the CylanceOPTICS agent	You install the CylanceOPTICS agent on Windows, macOS, and Linux devices. The agent deploys sensors to the device OS to monitor and collect data that is used to identify threats and trigger automated responses.

Data flow: Detecting and responding to events and storing event data (CylanceOPTICS 3.x and later)



1. An administrator uses the management console to configure detection rules and assigns the rules to a device policy.
2. The CylanceOPTICS cloud services send the detection rules over a secure WebSocket connection to a device with the CylanceOPTICS agent. The rule data also includes the configured responses for each event (for example, log off all users, suspend processes, and so on).
3. The CylanceOPTICS agent factors the detection rules into the Context Analysis Engine (CAE) that it uses to analyze and correlate events.
4. The CylanceOPTICS sensors detect an event.
5. The CAE determines whether the event satisfies a detection rule. If it does, one of the following occurs:
   - If the CylanceOPTICS agent is already configured with the event response, the agent executes the response.
   - If the agent requires additional data to execute the response (for example, if the response requires a playbook package that the device does not have yet), the agent sends the detection data to the CylanceOPTICS cloud services over a secure WebSocket connection. The CylanceOPTICS cloud services process the detection and provide the data that the agent requires to execute the response.
6. The agent prioritizes and sends the event data to the CylanceOPTICS cloud services over a dedicated event channel using a secure TLS connection. The CylanceOPTICS cloud services receive and process the event data, storing it in the secure CylanceOPTICS cloud database.
7. An administrator uses the management console to request detections data or to initiate an InstaQuery, advanced query, or focus view request. The management console interacts with the CylanceOPTICS cloud services using HTTP over TLS.
8. The CylanceOPTICS cloud services validate and process the request, retrieve the requested data from the CylanceOPTICS cloud database, and return the data to the management console.
9. The detection data, query result, or focus data is displayed in the management console.

What is CylanceGATEWAY?

CylanceGATEWAY is a cloud-native, artificial intelligence (AI) assisted Zero Trust Network Access (ZTNA) solution that gives your users access to your extended network perimeter and protects your extended network from threats. Organizations today face a challenging environment as cybersecurity threats become more sophisticated and pervasive while the number of connected enterprise endpoints and the amount of data sent to and stored in cloud services grows exponentially. CylanceGATEWAY provides network security while simultaneously enhancing and improving the network experience for end users. CylanceGATEWAY trusts nothing and no one by default. Every user, endpoint, and network are assumed to be potentially hostile, and no user can access anything until they prove who they are, that their access is authorized, that they're not acting maliciously, and that the local network they are connected to is not compromised.

CylanceGATEWAY protects users' iOS, Android, Windows 10, Windows 11, and macOS devices by allowing you to block connections to Internet destinations that you don't want devices to reach, even when the device isn't connected to your network. BlackBerry continually maintains an ever-growing list of unsafe Internet destinations that it can block endpoints from connecting to. If your organization also wants to block users from visiting specific sites that don't meet your acceptable use standards, you can create policies to specify additional destinations that all users or specific users or groups can't access.

Key features of CylanceGATEWAY

Feature	Description
Work Mode	Users can enable and disable Work Mode. Work Mode protects your network and devices. When enabled, each network access attempt is evaluated against the access control list (ACL) rules and specified network protection settings that are configured for your environment. The ACL defines allowed and blocked destinations on private and public networks. If allowed, the network traffic is sent through a secure tunnel to the CylanceGATEWAY cloud services.
Safe Mode support for macOS and Windows	You can enable Safe Mode for users. With Safe Mode, CylanceGATEWAY blocks apps and users from accessing potentially malicious destinations and enforces an acceptable use policy (AUP) by intercepting DNS requests. The CylanceGATEWAY cloud services evaluate each DNS query against the configured ACL rules and network protection settings (for example DNS Tunneling and Zero Day Detections such as Domain Generation Algorithm (DGA), Phishing, and Malware), and then instructs the agent to allow or block the request in real time. If allowed, the DNS request completes normally over the bearer network. Otherwise, the CylanceGATEWAY agent overrides the normal response to prevent access. **Note:** When enabled, Safe Mode will protect all DNS traffic that does not use the CylanceGATEWAY tunnel (for example, per-app tunnel access or split tunneling).
Start the agent or enable Work Mode automatically on macOS and Windows	In the Gateway Service policy, you can force the CylanceGATEWAY agent on macOS or Windows devices to automatically run when users log in or to automatically enable Work Mode when the agent starts. Your policy settings can override the "Start CylanceGATEWAY when I sign in" and "Enable Work Mode automatically" settings in the agent, but users can still manually enable and disable Work Mode after the agent starts or close the agent.

Feature	Description
Integrate with MDM solutions	You can connect Cylance Endpoint Security to BlackBerry UEM or Microsoft Intune so that Cylance Endpoint Security can verify whether iOS or Android devices are managed by UEM or Intune. You can specify whether devices must be UEM or Intune managed before they can use CylanceGATEWAY. For more information on network services, see Connecting Cylance Endpoint Security to MDM solutions to verify whether devices are managed.
Per-app tunnel access on macOS and iOS	On macOS and iOS devices under Mobile Device Management (MDM), you can designate which apps are allowed to use the CylanceGATEWAY Work Mode tunnel. You can use this to allow work use of bring-your-own-devices without extending the Work Mode access to all apps on a device.
Per-app tunnel support on Windows and Android	On Windows and Android devices, you can specify or restrict which apps can use the CylanceGATEWAY tunnel.
Continuous evaluation of network destinations	BlackBerry uses machine learning, IP reputation, and risk scoring to maintain an ever-evolving list of malicious Internet destinations. CylanceGATEWAY blocks devices from connecting to known and unknown phishing domains and associated IP and FQDN destinations, saving your organization the work of manually compiling and maintaining its own list.
Threat protection	CylanceGATEWAY uses machine learning to continuously protect your organization's network from threats by continuously monitoring network connections for potential threats. When an anomaly is identified, it is subsequently blocked or alerted upon based on the risk level that is set in the network protection settings. • Endpoints are protected against newly emerging network threats and established malicious destinations. Identified anomalies (for example, zero day, phishing domains, and command and control (C2) beacons) • DNS tunneling anomalies are detected based on CylanceGateway's analysis on the DNS traffic from the client to the attacker's DNS server.
Evaluate the risk level of a network destination	You can use the management console to evaluate the risk level and identify the category and subcategory of network destinations as they would be analyzed and determined by the CylanceGATEWAY cloud services.
Multiple private network support	You can deploy multiple CylanceGATEWAY Connectors from one Cylance Endpoint Security tenant to allow access to more than one of your private networks (for example, segments, data centers, and VPCs) which are both in an on-premises and cloud environment. You can view the CylanceGATEWAY Connectors that are associated with each specified Connector Group. You can create a maximum of eight connector groups and assign a maximum of eight CylanceGATEWAY Connectors to each group.

Feature	Description
Segmented private network access	You can install CylanceGATEWAY Connectors on-premises and on private cloud networks to provide network access to remote devices without changing network topology or routing, and without opening firewall holes for incoming traffic. Access through CylanceGATEWAY offers strong isolation; only the parts of the network you choose are exposed to endpoints, and endpoints are not exposed to the whole private network. The CylanceGATEWAY Connector can be deployed in an AWS, vSphere, ESXi, Microsoft Entra ID, or Hyper-V environment.
Monitor network access and traffic patterns	The CylanceGATEWAY dashboard in the management console displays multiple widgets that show connections, usage patterns, and alerts to help you monitor network traffic.
Specify network protection configurations	In the Network Protection screen, you can specify whether allowed network events (for example, Destination reputation and Signature detections) that are below the set minimum risk level are displayed as anomalies in the Network Events screen. If the allowed events are disabled, they are displayed as normal allowed traffic. Additionally, you can configure the SIEM solution or syslog support to only send blocked events. These features introduce more granular control over Network Protection and the SIEM solution or syslog and can help reduce alert fatigue.
Specify network protection settings to send to the Alerts view	In the Network Protection screen, you can specify the detections (for example, destination reputation, Signature detections, DNS Tunneling, and Zero Day) that you want to send to the Alerts view. Blocked and allowed ACL events are not shared to the Alerts view. This feature introduces more granular control over the alerts that are displayed in the Alerts view.
OS-specific ACL rules	You can create ACL rules and apply them to a specific OS. For example, you can allow access to some resources to only desktop devices (macOS and Windows).
One touch SaaS configuration	You can easily configure access to SaaS applications using the network services. CylanceGATEWAY streamlines SaaS app support and reduces the time required to enable SaaS app connectivity in the ACL rules that you configure for your environment. For more information on network services, see Define network services.
Content filtering	The ACL rules and the network protection settings that you configure for your environment filter the content and destinations that your users can access. This uses machine learning and ACL rules to ensure that users and devices comply with your organization's acceptable use and regulatory requirements.
NAT Details reporting	You can filter events based on the tunnel IP address (BlackBerry source IP) to identify the tunnel IP address used by users to access external destinations. The CylanceGATEWAY Connector provides additional information on UDP and TCP flows that flow through the tunnel to your private network after Network Address Translation (NAT) is applied (for example, Private NAT Source IP and Private Source Port). This allows you to identify the source IP address and the port number of an event that has been identified as potentially malicious or blocked and traverses your private network.

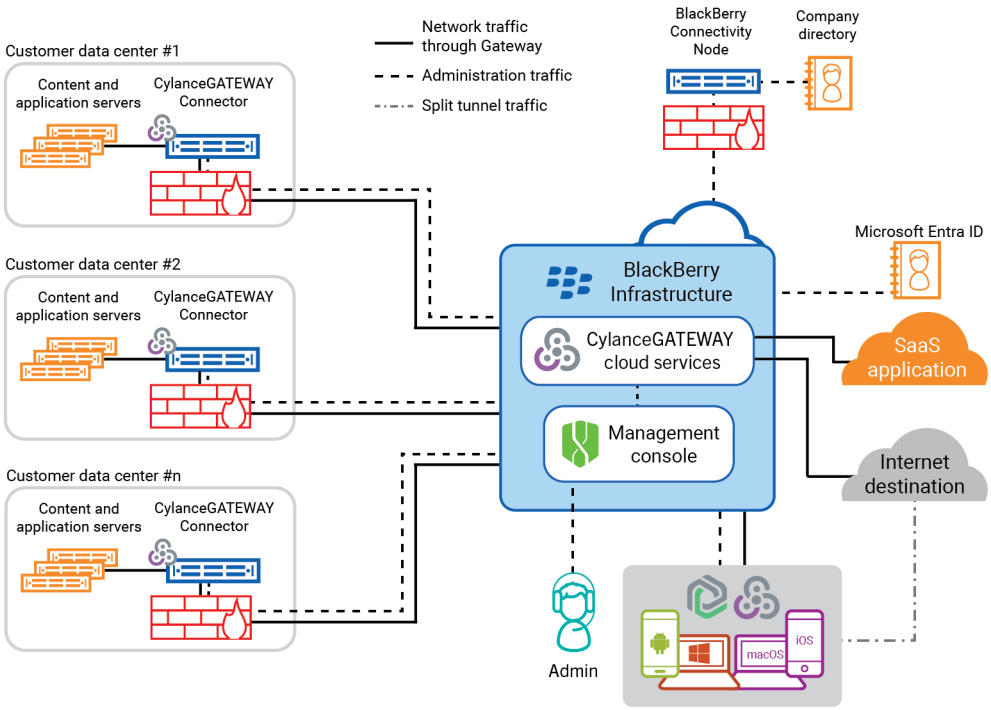
Feature	Description
Web access firewall	CylanceGATEWAY protects devices and your private networks by filtering, monitoring, and blocking traffic to potentially suspicious destinations. CylanceGATEWAY completes this by applying ACL rules that are configured for your environment and the network protection settings that you have specified. See the following for more information: • Monitoring network connections in the Administration content. • Controlling network access using ACL rules in the Setup content.
Support for IP-pinned services	Most SaaS applications allow source IP pinning to limit access only to connections from a specific range of trusted IP addresses. By limiting users to connections only through trusted entry points, organizations have an additional level of verification that the user is entitled to use the service. Your organization may already use this method to limit access to a SaaS application to connections from IP addresses used by devices connected to your organization's network. For users working remotely without using CylanceGATEWAY, this means that all traffic between remote devices and a SaaS application must travel over VPN to your network and then to the SaaS application. CylanceGATEWAY allows you to reserve CylanceGATEWAY IP addresses that are dedicated to your organization. You can use these IP addresses for source IP pinning in addition to your organization's IP addresses, providing the same level of security without requiring remote users to be connected to your organization's VPN.
Industry-leading tunnel technology	CylanceGATEWAY provides advanced layer 3 encryption for IP tunnels carrying TCP, UDP, ICMP, and real-time, low-latency traffic.
Android and iOS support	The CylancePROTECT Mobile app sends traffic through the tunnel to the CylanceGATEWAY cloud services and provides users with connection statistics, status information, and the ability to disable Work Mode and stop using CylanceGATEWAY for connections.
Windows 10, Windows 11, and macOS support	The CylanceGATEWAY agent that you install on devices sends traffic through the tunnel to the CylanceGATEWAY cloud services and provides users with connection statistics, status information, and the ability to disable Work Mode and stop using CylanceGATEWAY for connections.
Split tunneling	You can allow remote users to connect to safe public Internet sites directly over the Internet without tunneling through CylanceGATEWAY. When enabled, split DNS queries allow DNS lookups for the domains that are listed in the Private Network > DNS > Forward Lookup Zone configuration to be completed through the tunnel where network access controls are applied. All other DNS lookups are completed using your local DNS. If you enabled Safe Mode, DNS traffic that does not use the Gateway tunnel is protected by Safe Mode. Android and 64-bit Chromebook devices will use the tunnel where network access controls are applied.

Architecture: CylanceGATEWAY

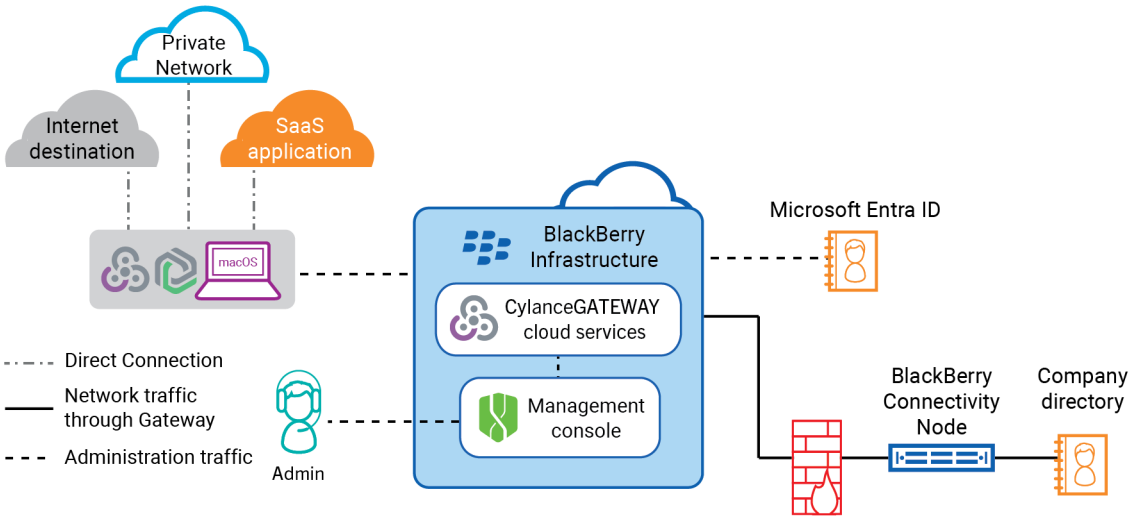
The CylanceGATEWAY architecture was designed to help you protect users' devices and your extended network from threats. The following diagrams show the architecture of CylanceGATEWAY in the two modes of operation.

- Work Mode: Work Mode creates a secure tunnel from devices, through the CylanceGATEWAY cloud services, to network resources and protects all of the traffic on that path.
- Safe Mode: Safe Mode extends the tenant's ACL rules and endpoint protection for macOS and Windows devices. When enabled, Safe Mode automatically takes effect when Work Mode is disabled, ensuring that devices are always protected.

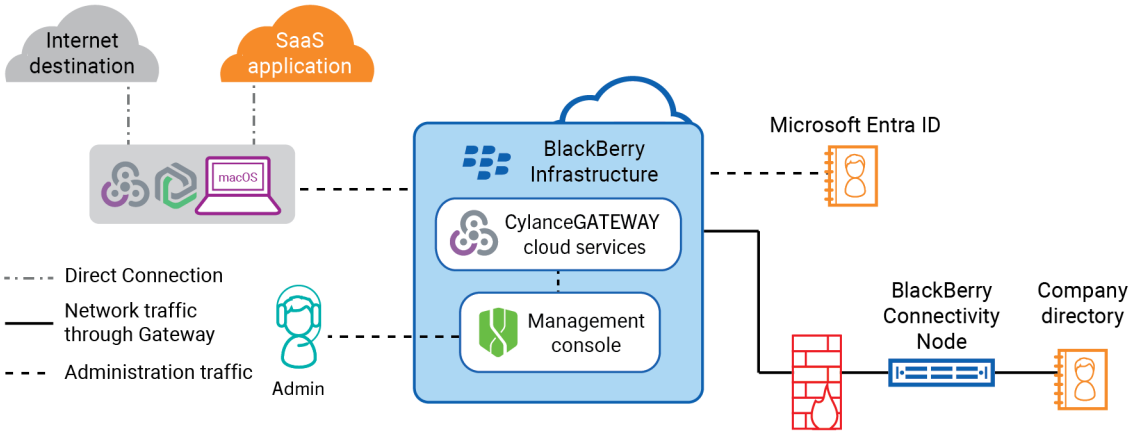
CylanceGATEWAY: Work Mode enabled



CylanceGATEWAY: Safe Mode enabled for users on the private network (for example, users in the office on the corporate network)



CylanceGATEWAY: Safe Mode enabled for users on a remote network (for example, a user is traveling)



Component	Description
CylanceGATEWAY cloud services	CylanceGATEWAY is a cloud-based service that provides Zero Trust Network Access to provide your users with access to your extended network perimeter and protect devices and your extended network from threats. The CylanceGATEWAY cloud services use machine learning to continuously evaluate network connections. Network anomaly events are detected when a CylanceGATEWAY user attempts to connect to a destination that might be suspicious or contain malicious content. Detected anomalies can block access to a destination based on the configured risk threshold for your environment.

Component	Description
Management console	The cloud-based management console allows you to configure, manage, and monitor CylanceGATEWAY and the connections made through it.
CylanceGATEWAY Connector	The CylanceGATEWAY Connector is an optional component that you can install behind your firewall and in private networks to establish a secure tunnel between the CylanceGATEWAY services and one of your private networks. The CylanceGATEWAY Connector allows users to communicate with content and application servers behind your firewall using CylanceGATEWAY instead of a traditional VPN.
BlackBerry Connectivity Node	The BlackBerry Connectivity Node is an optional component that allows Cylance Endpoint Security to synchronize users and groups with your on-premises Microsoft Active Directory or LDAP directory. Cylance Endpoint Security can synchronize users and groups with Microsoft Entra ID without the BlackBerry Connectivity Node.
Mobile devices with the CylancePROTECT Mobile app	CylanceGATEWAY supports iOS and Android devices. The CylancePROTECT Mobile app installed on mobile devices sends Internet traffic through a secure tunnel to the CylanceGATEWAY cloud services. Users can enable and disable work mode to specify whether data traffic uses the tunnel to the CylanceGATEWAY cloud services.
Desktop devices with the CylanceGATEWAY agent	CylanceGATEWAY supports macOS and Windows 10 and 11 devices. CylanceGATEWAY has two modes of operation: • With Work Mode, the CylanceGATEWAY agent sends network traffic through a secure tunnel to the CylanceGATEWAY cloud services. Users can enable and disable Work Mode to specify whether data traffic uses the tunnel. • With Safe Mode, CylanceGATEWAY blocks apps and users from accessing potentially malicious destinations and enforces an acceptable use policy (AUP) by intercepting DNS requests. The CylanceGATEWAY Cloud evaluates each DNS query against the configured ACL rules and network protection settings, and then instructs the agent to allow or block the request in real time. If allowed, the DNS request completes normally over the bearer network. Otherwise, the CylanceGATEWAY agent overrides the normal response to prevent access. When Safe Mode is enabled, users that are on the private network (for example, in the office) can access resources on your private network. Users on remote networks will not have access to resources on your private network.
SaaS applications	Software-as-a-Service applications provide cloud-based enterprise software, making apps and data available to users on multiple devices. Applications and data reside mostly on cloud-based servers managed by the vendor, easing deployment and reducing on-premises infrastructure costs, but requiring security measures that extend beyond firewalls and other perimeter-based security methods. CylanceGATEWAY can help secure user access to SaaS applications without requiring traffic to route through your organization's private network by enabling source IP pinning.

Component	Description
Internet destinations	Public Internet destinations include any web site, SaaS application, or other entity with an IP address that a client app can connect to over the Internet. BlackBerry maintains an ever-growing list of destinations that are known to be malicious. CylanceGATEWAY can block apps on devices from connecting to destinations on the list. If you enable split tunneling, traffic between devices and safe public sites that you specify can go directly over the Internet instead of through CylanceGATEWAY.

How CylanceGATEWAY sends data using Work Mode

When your users try to access destinations on the private network or any public Internet destination, they are only able to access them if they are explicitly allowed to by the access control list (ACL) rules. Each network access attempt is evaluated against the ACL rules and specified network protection settings that are configured for your environment. If an ACL rule blocks a destination, CylanceGATEWAY blocks the connection and doesn't route the traffic. If an ACL rule allows users to access the private network or a public Internet destination, the connection is re-evaluated every five minutes and the ACL rules are reapplied. If a user's risk level has changed or the destination reputation has been updated since the access attempt was established, the connection might be disconnected. When an ACL rule allows users to access a destination, the connection might be subsequently blocked or alerted on based on identified anomalies and the risk level that is set for the network protection settings.

- If a user's upload or download volume has changed, CylanceGATEWAY alerts of the unusual traffic pattern, but does not block the user's traffic.
- If the user tries to access a destination that is on BlackBerry's list of unsafe Internet destinations or newly identified as malicious, and your network protection risk threshold is set to high, the user's access will be blocked.

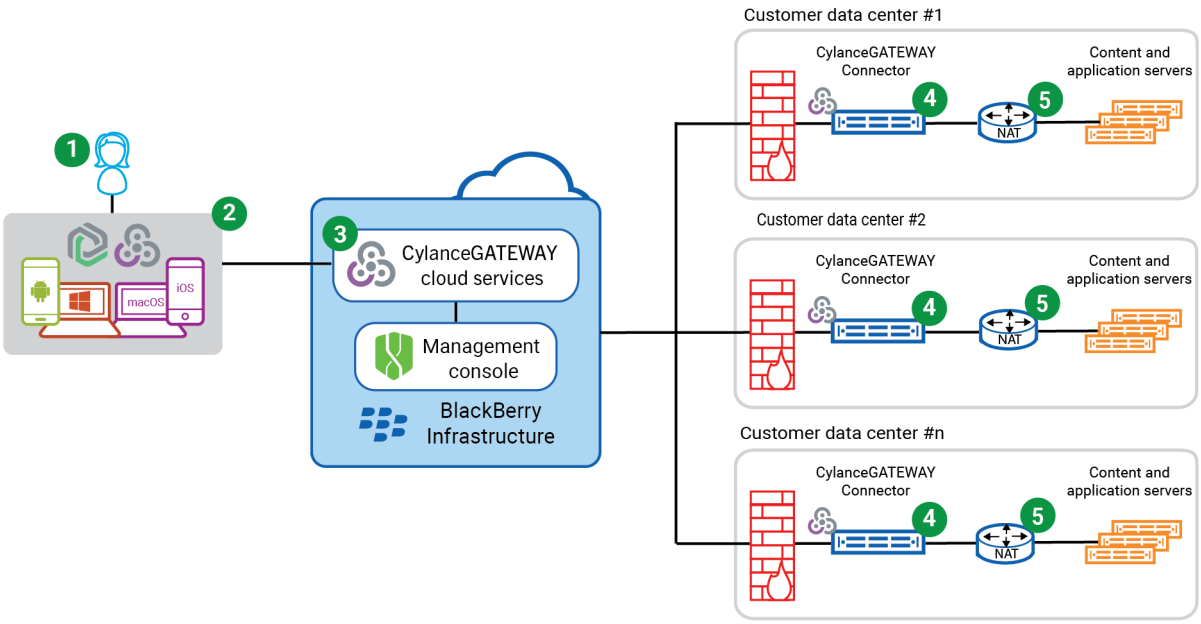
When CylanceGATEWAY is active on a device, CylanceGATEWAY routes network traffic in the following ways.

Destination	Action
Allowed destination on the private network	Users can access destinations on your private network only if they are explicitly allowed by the access control list (ACL) rules. ACL rules evaluate each network access attempt, and if a rule matches will allow access to the private network. All data between the device and your private network is encrypted using industry-leading tunnel technology and routed through secure tunnels from the CylancePROTECT Mobile app or CylanceGATEWAY agent to the BlackBerry Infrastructure and then from the BlackBerry Infrastructure to the CylanceGATEWAY Connector installed behind your firewall.

Destination	Action
Allowed Internet destination	Users can connect to any public Internet destination only if they are explicitly allowed by your ACL rules. ACL rules evaluate each network access attempt, and if a rule matches will allow access to the destination. Connections to public Internet destinations are routed through the secure tunnel between the CylancePROTECT Mobile app or CylanceGATEWAY Agent and the BlackBerry Infrastructure and then CylanceGATEWAY routes the traffic to the destination. If you enable split tunneling, traffic to safe Internet destinations is routed directly to the destination rather than through the tunnel to CylanceGATEWAY. For example, you can choose to reduce the traffic sent through CylanceGATEWAY by allowing traffic to safe public sites to route directly to the destination.
Allowed SaaS app	By default, connections to SaaS apps are routed in the same way as connections to other Internet destinations. If you enable source IP pinning, you can configure your SaaS app tenant to only accept connections from your organization's own IP addresses and CylanceGATEWAY.
Blocked destination on the private network	Users can access destinations on your private network only if they are explicitly allowed by the ACL rules. If the destination is not allowed, CylanceGATEWAY blocks the connection and doesn't route the traffic to the CylanceGATEWAY Connector. When users attempt to access a destination and it is blocked by an ACL rule, the attempt and reason is displayed on the Warning screen in the user's CylanceGATEWAY agent.
Blocked Internet destination	If a destination is explicitly blocked by your ACL rules or determined by BlackBerry to be a potentially malicious destination, CylanceGATEWAY will block the connection. When users attempt to access a destination and it is blocked by an ACL rule, the attempt and reason is displayed on the Warning screen in the user's CylanceGATEWAY agent.

Data flow: Accessing an application or content server on your private network

This data flow describes how data travels between devices and servers on your private networks using CylanceGATEWAY.

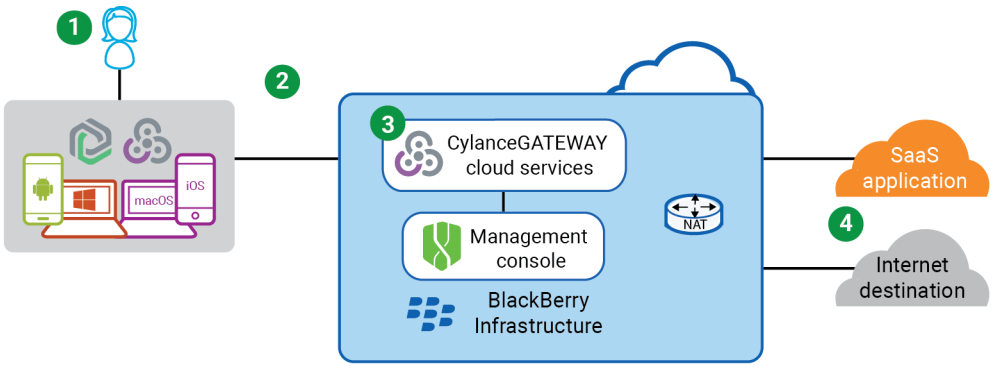


The above diagram shows the following sequence.

1. The user enables Work Mode and opens an app and attempts to access a resource on one of your private networks.
2. The CylancePROTECT Mobile app or the CylanceGATEWAY agent on the device routes the connection through a secure tunnel to CylanceGATEWAY in the BlackBerry Infrastructure.
3. CylanceGATEWAY performs the following actions:
   a. Determines, based on the access control list (ACL) rules, whether the user has access to that location on the private network.
   b. If the user has access, routes the connection through a secure tunnel to the CylanceGATEWAY Connector.
4. The CylanceGATEWAY Connector routes the connection to its destination on the private network.
5. The CylanceGATEWAY Connector applies Network Address Translation (NAT) to flows with a destination on your private network. The connector provides additional information on UDP and TCP flows allowing you to identify the source IP address and port number of an event that has been blocked or identified as potentially malicious. You cannot access the CylanceGATEWAY Connector endpoint from the private network using remote IT tools (for example, Remote Desktop Connection).

Data flow: Accessing a cloud-based application or Internet destination

This data flow describes how data travels between devices and a cloud-based SaaS application or public Internet destination using CylanceGATEWAY.



The above diagram shows the following sequence.

1. The user enables Work Mode and opens an app and attempts to access a cloud-based application or destination over the public Internet.
2. The CylancePROTECT Mobile app or the CylanceGATEWAY agent on the device sends the encrypted data through a secure tunnel to CylanceGATEWAY in the BlackBerry Infrastructure.
3. CylanceGATEWAY performs the following actions:
   a. Determines, based on the access control list (ACL) rules, whether the user has access to that location.
   b. If the user has access, sends the data to the SaaS application or allows access to the Internet destination.
   c. Applies Network Address Translation (NAT) to flows that access SaaS apps and Internet destinations by replacing the source IP address.
4. If source IP pinning is enabled, the SaaS application verifies that the connection is coming from an IP address that is associated with your CylanceGATEWAY tenant before allowing access.

How CylanceGATEWAY sends data using Safe Mode

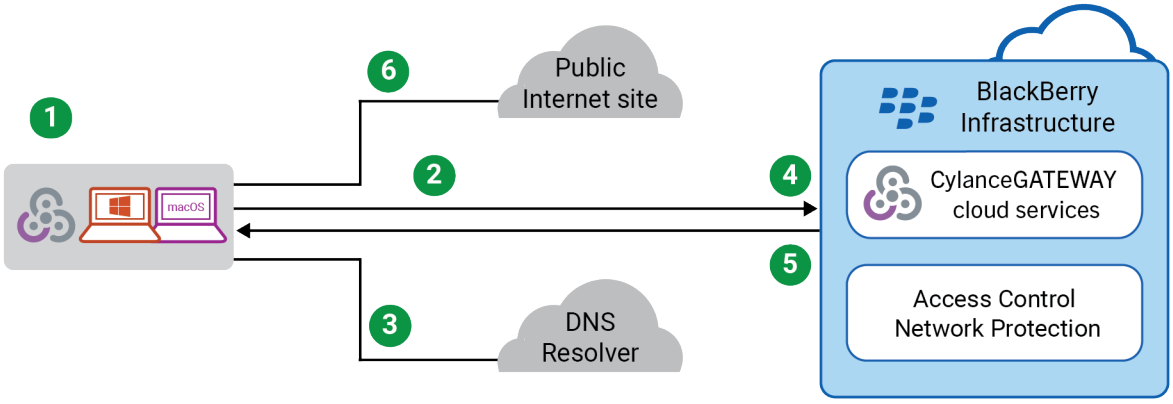
When your users try to access any public Internet destination, they are only able to access them if they are explicitly allowed to by the access control list (ACL) rules. When Safe Mode is enabled, CylanceGATEWAY blocks users from accessing potentially malicious destinations and enforces acceptable use policy (AUP) by intercepting DNS requests. The CylanceGATEWAY cloud services evaluate each DNS query against the configured ACL rules and network protection settings, and then instructs the agent to allow or block the request in real time. If the ACL rule blocks a destination, CylanceGATEWAY prevents access. If allowed, the network DNS query is allowed to complete over the bearer network.

When Safe Mode is enabled on a macOS or Windows device, CylanceGATEWAY sends network traffic in the following ways.

Destination	Action
Allowed Internet destination	Users can access any public Internet destination only if it is explicitly allowed by your ACL rules. ACL rules evaluate each network access attempt, and if a rule matches will allow access to the destination. If you enable Safe Mode, traffic to safe Internet destinations is routed over the bearer network to the destination instead of through the CylanceGATEWAY tunnel. If you enable split tunneling, traffic to safe Internet destinations is routed over the bearer network to the destination and is protected by Safe Mode. This reduces the traffic sent through CylanceGATEWAY by allowing traffic to safe public sites to route directly to the destination.
Blocked Internet destination	If a destination is explicitly blocked by your ACL rules or determined by BlackBerry to be a potentially malicious destination, CylanceGATEWAY will block the DNS query. When users attempt to access a destination and it is blocked by an ACL rule, the attempt and reason is displayed on the Warning screen in the user's CylanceGATEWAY agent.

Data flow: Accessing content, applications, and public Internet destinations using Safe Mode

This data flow describes how data travels between devices and a public Internet destination using Safe Mode. With Safe Mode, CylanceGATEWAY blocks apps and users from accessing potentially malicious destinations and enforces an acceptable use policy (AUP) by intercepting DNS requests. The CylanceGATEWAY cloud services evaluate each DNS query against the configured ACL rules and network protection settings, and then instructs the agent to allow or block the request in real time. If allowed, the DNS request completes normally over the bearer network. Otherwise, the CylanceGATEWAY agent overrides the normal response and prevents access.



The above diagram shows the following sequence.

1. The CylanceGATEWAY agent has Safe Mode enabled and the user attempts to access an Internet destination.
2. The CylanceGATEWAY agent intercepts the DNS request that is made from the device and queries the CylanceGATEWAY cloud services with information from that request.
3. The agent proxies the DNS request to the original DNS server.
4. The CylanceGATEWAY cloud services evaluate each query against the configured ACL rules and network protection settings, and then instructs the agent to allow or block the request.

5. If access is allowed, the agent proxies the original DNS server's response back as the response to the original DNS request. Otherwise, the agent injects a DNS response that blocks access.
6. The agent uses the results of an allowed DNS request to access an Internet destination.

What is CylanceAVERT?

CylanceAVERT is an information protection solution that detects and prevents the loss of sensitive regulatory and organizational information through external sources. CylanceAVERT can discover, categorize, and inventory sensitive company information and provide threat detection to prevent unauthorized exfiltration events. In addition to providing a sensitive file inventory and threat management, CylanceAVERT can scan files in the body content or the attachments of email messages, copied to a USB device, copied to a network drive, or uploaded to a browser location, and recommend a remediation action.

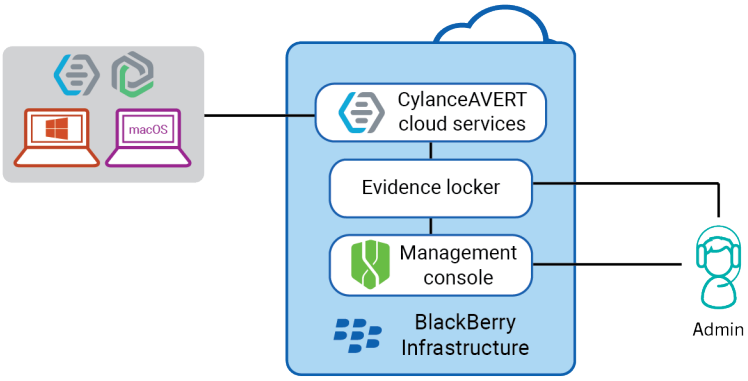
When a user attempts to upload sensitive data using a USB, browser domain, or in an email message, CylanceAVERT scans the content and determines if it is considered sensitive based on the information protection policies. The user will receive a warning if the policy has been violated and the configured remediation action will be applied.

Key features of CylanceAVERT

Feature	Description
Sensitive data scanning	CylanceAVERT can scan files uploaded to USB drives, internet browsers, and email attachments, as well as scan the body content of an email message for company data that the administrator defined as sensitive in the information protection policies. An email notification will be sent for data exfiltration events.
Information protection policies	You can specify the conditions that must be met to trigger the policy violation, the allowed domains for the policy, and the actions to take when a policy has been violated. See Managing information protection policies in the Cylance Endpoint Security Setup guide for more information.
CylanceAVERT events	You can create information protection policies to specify the data and conditions that must be met to trigger a policy violation, as well as the locations to apply the policy, the activities to monitor, and the remediation action to take when a policy has been violated. See CylanceAVERT events in the Cylance Endpoint Security Administration guide for more information.
Information protection settings	You can use the information protection settings to configure the sensitive data that they want to monitor for by adding templates and data types to use in an information protection policy. Administrators can also define the browser and email domains that will be allowed and trusted, manage the evidence that they want to collect for data exfiltration events, and specify how long the evidence should be available. Specified email addresses can also be sent notifications of data exfiltration events. See Define sensitive content using information protection settings in the Cylance Endpoint Security Setup guide for more information.
File inventory	The CylanceAVERT file inventory creates a record of all the sensitive files in an organization through a file trawling process. See Using the file inventory to identify sensitive files in the Cylance Endpoint Security Administration guide for more information.

Feature	Description
Evidence locker	You can use the evidence locker to view details of the files that have been involved in exfiltration events and download the files to their local storage for auditing purposes. See Using the evidence locker to view exfiltration event details in the Cylance Endpoint Security Administration guide for more information.

Architecture: CylanceAVERT



Item	Description
CylanceAVERT	CylanceAVERT prevents the loss of sensitive data from being exfiltrated through email messages and attachments, browser uploads, and USB devices.
Evidence locker	The evidence locker is a private file storage area that stores files involved in unauthorized exfiltration events for further inspection by administrators.
Management console	The cloud-based management console allows you to define the company sensitive data that you want to monitor and protect, manage user policies to specify the conditions that must be met to trigger an exfiltration event, view the sensitive files in your organization, and view various threat related events for risk assessment and remediation.
Devices with CylanceAVERT and CylancePROTECT	CylancePROTECT Desktop must be installed on the endpoint to utilize CylanceAVERT functionality. CylanceAVERT supports Windows 10 and 11.

Legal notice

©2024 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

Patents, as applicable, identified at: www.blackberry.com/patents.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES

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