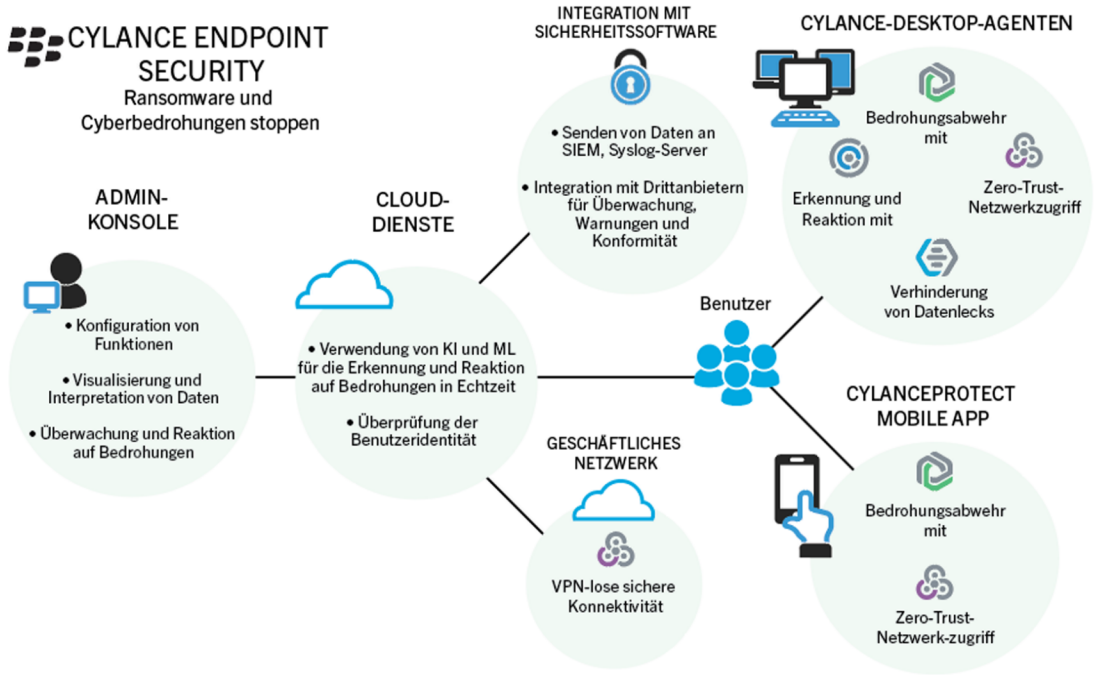
Cylance Endpoint Security

Überblick und Architektur

Contents

Was ist Cylance Endpoint Security?



Cylance Endpoint Security bietet eine einheitliche Endpunktsicherheitslösung, die für die neuen Gegebenheiten entwickelt wurde. Es führt die besten verfügbaren KI-basierten Tools zur Erkennung, zum Schutz und zur Beseitigung von Bedrohungen auf jedem Endpunkt zusammen. Cyberkriminelle nutzen heute künstliche Intelligenz (KI), um zunehmend hochentwickelte Bedrohungen zu schaffen, die die Reichweite und Wirkung ihrer Angriffe maximieren. Daher müssen sich auch die heutigen Lösungen die Vorteile von maschinellem Lernen und KI zunutze machen. Cylance Endpoint Security stellt eine KI-gestützte Zero-Trust-Lösung für alle Geräte, Netzwerke, Apps und Mitarbeiter bereit.

Mit dem Zero-Trust-Ansatz wird die Netzwerksicherheit modernisiert und gleichzeitig das Netzwerkerlebnis für Endbenutzer verbessert. Das Zero-Trust-Sicherheitsmodell vertraut standardmäßig nichts und niemandem, einschließlich Benutzern im geschäftlichen Netzwerk. Jeder Benutzer, jeder Endpunkt und jedes Netzwerk wird als potenziell gefährlich angesehen. Bei Zero-Trust-Sicherheit kann ein Benutzer erst auf alles zugreifen, wenn er nachgewiesen hat, wer er ist, dass sein Zugriff autorisiert ist, dass das Netzwerk, mit dem er verbunden ist, nicht gefährdet ist und dass er oder sich auf seinem Gerät befindliche Malware nicht böswillig handelt.

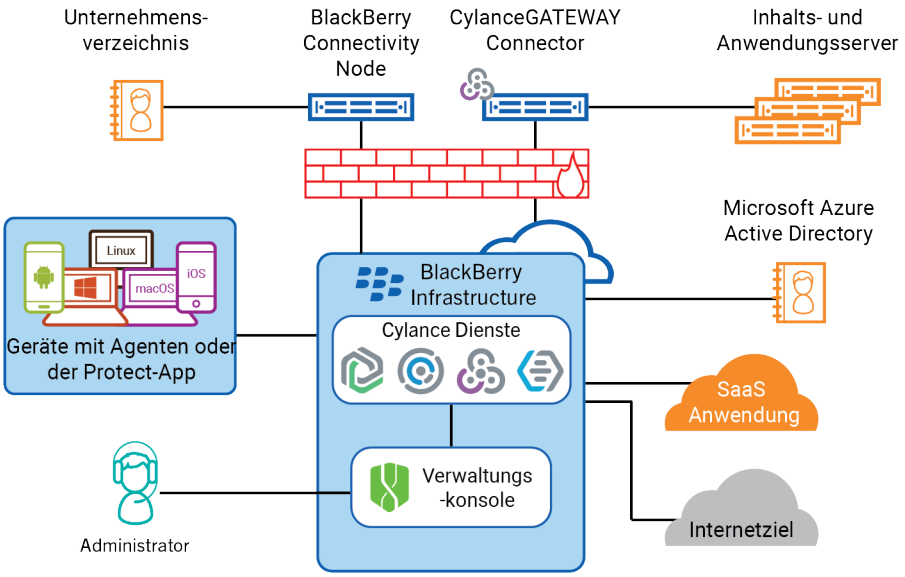
Wichtige Funktionen von Cylance Endpoint Security

Cylance Endpoint Security bietet eine breite Palette an Sicherheitsfunktionen über mehrere miteinander verbundene Funktionen:

Funktion	Beschreibung
Erkennen und Blockieren von Ransomware, Malware und anderen Bedrohungen	CylancePROTECT Desktop blockiert Ransomware und andere Malware auf Windows-, macOS- und Linux-Geräten mithilfe eines mathematischen Ansatzes zur Malware-Identifizierung. Es verwendet Techniken des maschinellen Lernens anstelle von reaktiven Signaturen, vertrauenswürdigen Systemen oder Sandboxes, um Endpunkterkennung und Reaktionen bereitzustellen, durch die neue Ransomware, Malware, Viren, Bots und zukünftige Varianten unschädlich gemacht werden. CylancePROTECT Desktop analysiert potenzielle Dateiausführungen auf Ransomware und andere Malware auf den Betriebssystem- und Speicherebenen, um die Bereitstellung schädlicher Payloads zu verhindern.
Schutz für Mobilgeräte	CylancePROTECT Mobile bietet Schutz vor mobilen Bedrohungen für iOS-, Android- und Chrome OS-Geräte. Zusätzlich zur Malware-Erkennung erkennt CylancePROTECT Mobile auch Sideloading-Apps, schädliche URLs in Textnachrichten und andere Sicherheitsrisiken und empfiehlt spezifische Maßnahmen zur Beseitigung der Bedrohung.
Erkennung von und Reaktion auf Angriffe	CylanceOPTICS überwacht Ihre Windows-, macOS- und Linux-Geräte und informiert Sie über mögliche Angriffe auf Ihr Unternehmen. CylanceOPTICS sammelt Informationen von Geräten und aggregiert sie mithilfe der Cloud-Dienste, um schädliche Ereignisse zu verfolgen, vor diesen zu warnen und sofort darauf zu reagieren. CylanceOPTICS kann Angriffe stoppen, bevor sie ausgeführt werden, und die Untersuchung und Reaktion auf Angriffe automatisieren.
Sicherer Zugriff auf Ihr Netzwerk und Ihre Cloud-basierten Dienste	CylanceGATEWAY bietet Zero-Trust-Netzwerkzugriff (ZTNA) für die iOS-, Android-, Windows- - und macOS-Geräte Ihrer Benutzer, um den Benutzerzugriff auf Ihre erweiterte Netzwerkumgebung zu sichern und Ihr erweitertes Netzwerk vor Bedrohungen zu schützen CylanceGATEWAY schützt Geräte, indem es Ihnen ermöglicht, Verbindungen zu Internetzielen zu blockieren, mit denen die Geräte keine Verbindung aufnehmen sollen, auch wenn das Gerät nicht mit Ihrem Netzwerk verbunden ist. CylanceGATEWAY schützt Ihr privates Netzwerk und Ihre Cloud-basierten Dienste, indem nur autorisierte Benutzer Zugriff erhalten.
Schutz sensibler Daten	CylanceAVERT identifiziert und kategorisiert sensible Daten auf Windows-Geräten in Ihrer Unternehmensumgebung, um eine Bestandsaufnahme sensibler Dateien zu erstellen und bestimmte Benutzer zu benachrichtigen, wenn sensible Daten an einem Exfiltrationsereignis beteiligt sind. CylanceAVERT kann Dateien scannen, die auf ein USB-Gerät kopiert, auf einen Browser-Speicherort oder ein Netzlaufwerk hochgeladen oder im Text oder in den Anhängen von E-Mail-Nachrichten gespeichert wurden, und eine Korrekturmaßnahme empfehlen.

Funktion	Beschreibung
Zusammenarbeit mit beliebigen UEM- bzw. MDM-Plattformen	Cylance Endpoint Security kann mit BlackBerry UEM verwendet werden, um ein Höchstmaß an Endpunktverwaltung und Sicherheit zu bieten und Ihr Unternehmen vor einer Vielzahl von Bedrohungen zu schützen. Wenn Sie über eine andere Unified Endpoint Management (UEM)- oder Mobile Device Management (MDM)-Plattform als BlackBerry UEM verfügen, können Sie Cylance Endpoint Security verwenden, um Ihre Endpunkte und die zwischen ihnen und Ihrem Netzwerk übertragenen Daten besser zu schützen. Im Laufe der Zeit werden spezifische Integrationen mit MDM-Lösungen wie UEM und Microsoft Intune zu Cylance Endpoint Security hinzugefügt, die die Verwaltungsmöglichkeiten für Geräte als Reaktion auf potenzielle Bedrohungen weiter verbessern.

Cylance Endpoint Security-Architektur



Komponente	Beschreibung
BlackBerry Infrastructure	Die BlackBerry Infrastructure ist ein globales privates Datennetzwerk, das über mehrere Regionen verteilt ist und die Datenübertragung zwischen Tausenden von Unternehmen und Millionen von Benutzern weltweit ermöglicht und sichert. Sie ist darauf ausgelegt, den Transport von Daten zwischen BlackBerry-Diensten und Endbenutzergeräten effizient zu verwalten. Die BlackBerry Infrastructure registriert Benutzerinformationen für die Agenten- und CylancePROTECT Mobile-App-Aktivierung, validiert Lizenzinformationen und erhält eine vertrauenswürdige Verbindung mit lokalen Komponenten aufrecht, die hinter der Firewall installiert sind, und mit Agenten und der CylancePROTECT Mobile-App auf Benutzergeräten innerhalb und außerhalb der Firewall.

Komponente	Beschreibung
CylancePROTECT	CylancePROTECT Desktop erkennt und blockiert Malware auf Windows-, macOS- und Linux-Geräten mithilfe von Techniken des maschinellen Lernens, um neue Malware, Viren, Bots und zukünftige Varianten unschädlich zu machen. CylancePROTECT Mobile erkennt Malware, Sideloading-Apps, schädliche URLs in Textnachrichten und andere Sicherheitsrisiken auf iOS-, Android- und Chrome OS-Geräten und empfiehlt Maßnahmen zur Beseitigung der Bedrohung.
CylanceOPTICS	CylanceOPTICS überwacht Windows-, macOS- und Linux-Geräte und aggregiert erfasste Informationen, um schädliche Ereignisse zu erkennen und zu verfolgen, vor ihnen zu warnen und darauf zu reagieren, sobald sie auftreten. CylanceOPTICS kann dazu beitragen, beginnende Angriffe zu erkennen und Untersuchungen und Reaktionen zu automatisieren, sodass Angriffe gestoppt werden, bevor sie Schaden anrichten.
CylanceGATEWAY	CylanceGATEWAY schützt den Netzwerkzugriff für das private Netzwerk Ihres Unternehmens und Cloud-basierte Anwendungen, die Ihren Windows-, macOS-, iOS- und Android-Benutzern Zugriff auf Ihre erweiterte Netzwerkumgebung ermöglichen, und schützt Ihr erweitertes Netzwerk vor Bedrohungen.
CylanceAVERT	CylanceAVERT erkennt und verhindert den Verlust sensibler regulatorischer und organisatorischer Informationen über externe Quellen. CylanceAVERT kann vertrauliche Unternehmensinformationen erkennen, kategorisieren und inventarisieren und Bedrohungserkennung bereitstellen, um nicht autorisierte Exfiltrationsereignisse zu verhindern.
Cylance Endpoint Security-Cloud-Dienste	Die Cylance Endpoint Security-Cloud-Dienste stellen die Intelligenz hinter jeder Cylance Endpoint Security-Funktion bereit. Die Cloud-Dienste für verschiedene Funktionen nutzen KI, maschinelles Lernen und eine Risiko-Engine auf Basis von Benutzermodellen, um große Mengen komplexer Daten zu verarbeiten und Bedrohungen zu erkennen und darauf zu reagieren. Weitere Informationen finden Sie unter So nutzt Cylance Endpoint Security zum Schutz von Benutzern und Geräten modernste Technologie.
Verwaltungskonsole	Mit der Cloud-basierten Verwaltungskonsole können Sie alle Funktionen von Cylance Endpoint Security einrichten, verwalten und überwachen.
Geräte mit Agenten oder der CylancePROTECT Mobile-App	Auf Windows-, macOS- und Linux-Geräten installierte Agenten und die auf iOS-, Android- und Chrome OS-Geräten installierte CylancePROTECT Mobile-App kommunizieren mit Cylance Endpoint Security, um potenzielle Bedrohungen zu erkennen und Maßnahmen zum Schutz Ihrer Benutzer und Geräte sowie Ihres Netzwerks zu ergreifen.
BlackBerry Connectivity Node	BlackBerry Connectivity Node ist eine optionale Komponente, mit der Cylance Endpoint Security Benutzer und Gruppen mit Ihrem lokalen Microsoft Active Directory oder LDAP-Verzeichnis synchronisieren kann. Cylance Endpoint Security kann Benutzer und Gruppen mit Entra Active Directory ohne Verwendung von BlackBerry Connectivity Node synchronisieren.

Komponente	Beschreibung
CylanceGATEWAY Connector	Der CylanceGATEWAY Connector ist eine optionale Komponente, die Sie hinter der Firewall und in privaten Cloud-Netzwerken installieren können, um einen sicheren Tunnel zwischen der BlackBerry Infrastructure und dem privaten Netzwerk einzurichten. Der CylanceGATEWAY Connector ermöglicht Benutzern die Kommunikation mit Inhalts- und Anwendungsservern hinter der Firewall über CylanceGATEWAY statt über ein herkömmliches VPN.

So nutzt Cylance Endpoint Security zum Schutz von Benutzern und Geräten modernste Technologie

CylancePROTECT Desktop und CylancePROTECT Mobile nutzen hochmoderne Cloud-Dienste, um zu ermitteln, ob Software, Dateien und Websites potenziell schädlich sind und eine Bedrohung für die Sicherheit eines Geräts darstellen. Die CylancePROTECT-Cloud-Dienste verwenden ausgeklügelte KI, maschinelles Lernen und effiziente mathematische Modelle, um große Datenmengen aus globalen Quellen zu verarbeiten, zu speichern und kontinuierlich aus den Mustern und Eigenschaften dieser Daten zu lernen. Diese Daten werden genutzt, um intelligente Prognosen und Entscheidungen über das Risikopotenzial von Software, Dateien und Internetzielen in nahezu Echtzeit zu treffen. Die CylancePROTECT-Dienste werden ständig weiterentwickelt, um neue Cyberbedrohungen zu bewältigen. Sie bieten eine aggressive und proaktive Sicherheitsstrategie, die schädliche Software und Webseiten identifiziert, bevor sie sich auf die Infrastruktur oder die Gerätebenutzer Ihres Unternehmens auswirken können.

Die CylancePROTECT-Dienste bieten die Bedrohungsanalyse für Dateien, die vom CylancePROTECT Desktop-Agenten gescannt werden. Wenn eine Datei als bösartig identifiziert wird, führt der CylancePROTECT Desktop-Agent alle von Ihnen konfigurierten Maßnahmen zur Risikominderung durch (z. B. Warnung oder Quarantäne). Der Agent enthält ein lokales CylancePROTECT-Dienstmodell. Wenn der Agent nicht mit der Cloud kommunizieren kann, wird das lokale Modell für die Dateibewertung verwendet.

CylanceGATEWAY bietet Modelle für maschinelles Lernen (z. B. Signaturerkennung und DNS-Tunneling-Erkennung) sowie kontinuierliche Überwachung und dynamische Anwendung von IP-Reputationsdatenbanken, um den Netzwerkverkehr zu überwachen und Ziele zu identifizieren, die potenziell schädliche Bedrohungen enthalten könnten. Wenn ein Ziel als potenzielle Bedrohung identifiziert wird, führt CylanceGATEWAY alle von Ihnen konfigurierten Aktionen aus (z. B. Benachrichtigung oder Blockierung der Verbindung zu den Zielen). CylanceGATEWAY bietet zwei Betriebsmodi (Arbeitsmodus und Sicherheitsmodus), mit denen die Geräte der Benutzer und Ihr Netzwerk vor Bedrohungen geschützt sind.

Die CylancePROTECT-Dienste sind eine Kernkomponente verschiedener CylancePROTECT Mobile-Funktionen, darunter Malware-Erkennung, SMS-Nachrichten-Scans und sichere Netzwerkprüfungen. Wenn CylanceGATEWAY aktiviert ist, verwendet die CylancePROTECT Mobile-App auch maschinelles Lernen, um den Netzwerkverkehr kontinuierlich zu überwachen, und kann den Zugriff eines Benutzers auf ein Ziel blockieren.

Der CylanceOPTICS-Agent auf Desktop-Geräten sendet die erfassten Daten an die CylanceOPTICS-Cloud-Dienste. Die Daten werden aggregiert und in der sicheren CylanceOPTICS-Cloud-Datenbank gespeichert. Die CylanceOPTICS-Datenanalysedienste bieten umfassende Interpretationen von Gerätedaten, auf die Sie in der Verwaltungskonsole zugreifen können. CylanceOPTICS verwendet eine Kontextanalyse-Engine (Context Analysis Engine, CAE), um auf Geräten auftretende Ereignisse zu analysieren und korrelieren. Sie können CylanceOPTICS so konfigurieren, dass automatische Antwortaktionen durchgeführt werden, wenn die CAE bestimmte Artefakte von Interesse erkennt (z. B. Anzeigen einer Benachrichtigung oder Abmelden des aktuellen Benutzers), und eine zusätzliche Ebene zur Erkennung und Prävention von Bedrohungen geboten wird, um die Funktionen von CylancePROTECT Desktop zu ergänzen.

Der CylanceGATEWAY-Agent auf Desktop-Geräten verwendet maschinelles Lernen und statische Reputationsdatenbanken, um Ziele mit potenziell schädlichen Bedrohungen zu identifizieren. Wenn der Agent auch für den Sicherheitsmodus aktiviert ist und diesen verwendet, wendet CylanceGATEWAY eine Richtlinie für die zulässige Nutzung (UAP) an und fängt jede DNS-Abfrage ab, um zu bestimmen, ob die Verbindung fortgesetzt werden kann oder blockiert werden muss.

Der CylanceAVERT-Agent identifiziert die sensiblen Dateien auf einem Endpunkt und benachrichtigt den Administrator über jeden Versuch, diese Dateien per E-Mail, Browser-Uploads, über Netzlaufwerke oder USB-Geräte zu exportieren. Wenn eine sensible Datei an einem Exfiltrationsereignis beteiligt ist, führt CylanceAVERT die vom Administrator in den Einstellungen zum Schutz von Informationen angegebene Maßnahme zur Risikominderung aus. CylanceAVERT verwendet Schlüsselwortabgleich und Regex-Validierung, um die sensiblen Datentypen zu identifizieren, die ein Exfiltrationsereignis auslösen.

Was ist CylancePROTECT Desktop?

CylancePROTECT Desktop erkennt und blockiert Malware, bevor diese Geräte beeinträchtigen kann. BlackBerry verwendet einen mathematischen Ansatz zur Malware-Identifizierung, wobei maschinelles Lernen anstelle von reaktiven Signaturen, vertrauensbasierten Systemen oder Sandboxes verwendet wird. Dieser Ansatz macht neue Malware, Viren, Bots und zukünftige Varianten unschädlich. CylancePROTECT Desktop analysiert potenzielle Dateiausführungen auf Malware in den Betriebssystem- und Speicherschichten, um die Bereitstellung schädlicher Payloads zu verhindern.

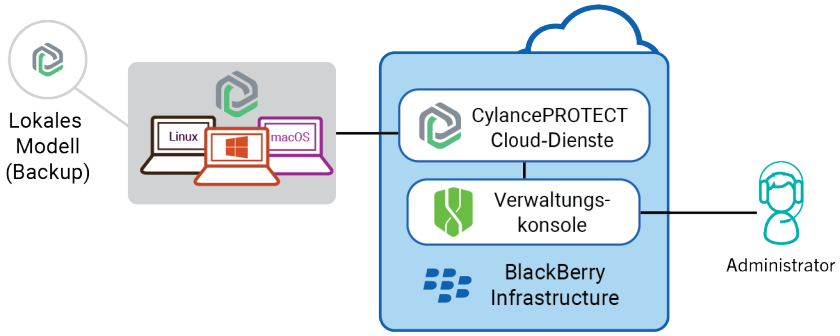
Der CylancePROTECT Desktop-Agent ist so konzipiert, dass er nur eine minimale Menge an Systemressourcen verbraucht. Der Agent behandelt Dateien oder Prozesse, die ausgeführt werden, mit hoher Priorität, da diese Ereignisse bösartig sein können. Dateien, die einfach auf der Festplatte abgelegt sind (gespeichert sind, aber nicht ausgeführt werden), haben eine niedrigere Priorität, da sie zwar schädlich sein können, aber keine unmittelbare Bedrohung darstellen.

Wichtige Funktionen von CylancePROTECT Desktop

Funktion	Beschreibung
Erkennen und unter Quarantäne stellen von schädlichen Dateien	CylancePROTECT Desktop bietet Optionen für die Handhabung von Dateien, die als unsicher oder anormal erkannt werden. Sie können Dateien, die in Bedrohungsereignissen identifiziert wurden, einer Quarantäneliste oder einer sicheren Liste hinzufügen, um zukünftige Ereignisse besser handhaben zu können.
Schutz vor Speicher-Exploits	CylancePROTECT Desktop bietet Optionen für die Handhabung von Speicher-Exploits einschließlich Prozessinjektionen und Berechtigungseskalationen. Sie können auch ausführbare Dateien zu einer Ausschlussliste hinzufügen, sodass diese Dateien ausgeführt werden können, wenn eine Geräterichtlinie angewendet wird.
Blockieren schädlicher Skripte	CylancePROTECT Desktop überwacht und schützt vor schädlichen Skripten, die in Ihrer Umgebung ausgeführt werden. Der CylancePROTECT Desktop-Agent kann das Skript und den Skriptpfad erkennen, bevor das Skript ausgeführt wird, und es blockieren.
Blockieren von Bedrohungen von USB-Speichergeräten	CylancePROTECT Desktop steuert, wie USB-Massenspeichergeräte mit Geräten in Ihrem Unternehmen verbunden werden können. Sie können USB-Massenspeichergeräte einschließlich USB-Flash-Laufwerken, externe Festplatten und Smartphones zulassen oder blockieren.
Empfangen sofortiger Warnungen	CylancePROTECT Desktop überwacht die Ausführung schädlicher Prozesse und warnt Sie, wenn unsichere oder anormale Ausführungsversuche unternommen werden.
Erkennen inaktiver Geräte	Wenn der CylancePROTECT Desktop-Agent über einen bestimmten Zeitraum keinen Kontakt mehr hat, wird der Gerätestatus auf „Inaktiv“ geändert. Sie können inaktive Geräte überprüfen, um festzustellen, ob sie von der Verwaltungskonsole entfernt werden sollten.

Funktion	Beschreibung
Schutz virtueller Maschinen	CylancePROTECT Desktop ist pro Gast weniger ressourcenintensiv, da die Technologie keine täglichen Datenträgerscans erfordert. CylancePROTECT Desktop ist pro Gast auch weniger arbeitsspeicherintensiv.

Architektur: CylancePROTECT Desktop



Element	Beschreibung
CylancePROTECT-Cloud-Dienste	CylancePROTECT Desktop erkennt und blockiert Malware mithilfe von Techniken des maschinellen Lernens, um neue Malware, Viren, Bots und zukünftige Varianten unschädlich zu machen. Die CylancePROTECT-Cloud-Dienste verwenden ausgeklügelte KI, maschinelles Lernen und effiziente mathematische Modelle, um große Datenmengen aus globalen Quellen zu verarbeiten, zu speichern und kontinuierlich aus den Mustern und Eigenschaften dieser Daten zu lernen. Diese Daten werden genutzt, um intelligente Prognosen und Entscheidungen über das Risikopotenzial von Software, Dateien und Internetzielen in nahezu Echtzeit zu treffen. Die CylancePROTECT-Dienste stellen die Bedrohungsbewertung für Dateien bereit, die vom CylancePROTECT Desktop-Agenten gescannt werden. Die Dateibewertung bestimmt basierend auf der dem Agenten zugewiesenen Geräterichtlinie, welche Aktion der Agent für die Datei durchführen soll.
Verwaltungskonsole	Mit der Cloud-basierten Verwaltungskonsole können Sie verschiedene Ereignisse mit Bedrohungsbezug anzeigen, Geräterichtlinien zur Konfiguration von Agenten auf Endpunkten verwalten und globale Listen für unter Quarantäne gestellte und sichere Dateien bearbeiten.
Geräte mit dem CylancePROTECT Desktop-Agenten	Der CylancePROTECT Desktop-Agent muss auf einem Gerät (Endpunkt) installiert werden, um das Gerät zu schützen. CylancePROTECT Desktop unterstützt Windows-, macOS- und Linux-Betriebssysteme.

Element	Beschreibung
Lokales Modell	Der CylancePROTECT Desktop-Agent verwaltet auf jedem Endpunkt eine sekundäre Kopie des Modells, die von den CylancePROTECT-Diensten zur Bewertung von Dateien verwendet wird. Wenn der Agent keine Verbindung zu den CylancePROTECT-Diensten herstellen kann, berechnet das lokale Modell die Dateibewertungen.

Was ist CylancePROTECT Mobile?

CylancePROTECT Mobile ist eine fortschrittliche Sicherheitslösung, die Cyberbedrohungen auf iOS-, Android- und Chrome OS-Geräten proaktiv in Echtzeit erkennt und verhindert, ohne die Produktivität Ihrer Mitarbeiter zu beeinträchtigen.

CylancePROTECT Mobile verwendet eine Kombination aus Spitzentechnologien:

- Die webbasierte Verwaltungskonsole, mit der Sie mobile Geräte und CylancePROTECT Mobile-Funktionen verwalten und Details zu mobilen Bedrohungen anzeigen können.
- Die CylancePROTECT Mobile-App, die das Gerät eines Benutzers in regelmäßigen Abständen scannt, um Bedrohungen zu erkennen und eine allgemeine Sicherheitsbewertung durchzuführen. Wenn möglich, gibt die App dem Benutzer klare Anweisungen zur Lösung von Bedrohungen, ohne dass der Administrator eingreifen muss.
- Die CylancePROTECT-Cloud-Dienste, die ausgeklügelte KI und maschinelles Lernen verwenden, um wichtige CylancePROTECT Mobile-Funktionen zu unterstützen, einschließlich der Echtzeitidentifizierung von Malware und unsicheren URLs in Textnachrichten.

Durch die nahtlose Integration dieser Technologien wird ein sicheres Ökosystem geschaffen, in dem Daten geschützt und schädliche Aktivitäten auf mobilen Geräten identifiziert und proaktiv beseitigt werden. CylancePROTECT Mobile ist einfach zu konfigurieren, für Endbenutzer leicht zu verstehen und zu verwenden und nutzt Cloud-Technologien, die sich ständig verbessern und intelligenter werden.

Wichtige Funktionen von CylancePROTECT Mobile

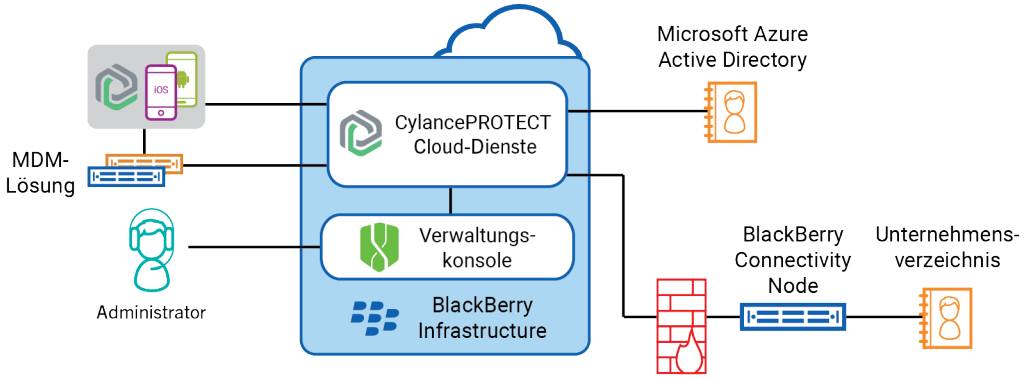
Funktion	Beschreibung
Malware-Erkennung für Android-Geräte	Die CylancePROTECT Mobile-App kann Malware auf Android-Geräten erkennen und den Benutzer anweisen, schädliche Apps zu deinstallieren. Die CylancePROTECT Mobile-App scannt die Apps auf dem Gerät eines Benutzers und lädt die App-Dateien in die CylancePROTECT-Cloud-Dienste hoch, die KI und maschinelles Lernen verwenden, um das App-Paket zu analysieren und eine Zuverlässigkeitsbewertung zu erzeugen, die an die CylancePROTECT Mobile-App zurückgegeben wird. Die Zuverlässigkeitsbewertung bestimmt, ob die gescannte App sicher oder potenziell schädlich ist. Wenn von den CylancePROTECT-Diensten festgestellt wird, dass eine App potenziell schädlich ist, benachrichtigt die App den Benutzer und gibt weitere Details an. Der Benutzer kann auf eine Korrekturoption in der App tippen, um zu den Geräteeinstellungen zu navigieren und die schädliche App zu deinstallieren. Wenn eine App einen Hash enthält, den die Dienste zuvor noch nicht verarbeitet haben, wird sie zu den CylancePROTECT-Diensten hochgeladen. Wenn der Gerätescan eine App findet, die zuvor analysiert wurde, verwendet er die Zuverlässigkeitsbewertung, die die CylancePROTECT-Dienste bereits für diesen eindeutigen App-Hash generiert haben. Wenn eine App einen neuen Hash hat (z. B. für eine neue Version), wird die App zur Analyse und Bewertung zu den CylancePROTECT-Diensten hochgeladen (sofern sie nicht bereits von einem anderen Gerät hochgeladen worden ist).

Funktion	Beschreibung
Sideload-Erkennung für iOS- und Android-Geräte	Sideloading-Apps unterliegen nicht denselben Einschränkungen oder Schutzmechanismen wie Apps, die über offizielle App Stores verteilt werden. Die CylancePROTECT Mobile-App kann das Vorhandensein einer Sideloading-App auf dem Gerät eines Benutzers erkennen, den Benutzer benachrichtigen und ihn anweisen, sie zu deinstallieren. Bei iOS kann die CylancePROTECT Mobile-App nur Sideloading-App-Entwicklerzertifikate erkennen, für die der Benutzer in den Geräteeinstellungen angegeben hat, dass er ihnen vertraut. Benutzer können Sideloading-Apps nur verwenden, wenn das App-Entwicklerzertifikat als vertrauenswürdig eingestuft wird. Bei Android identifiziert die CylancePROTECT Mobile-App Sideloading-Apps auf der Basis der Installationsquelle. Die CylancePROTECT-Cloud-Dienste und die CylancePROTECT Mobile-App betrachten offizielle App-Quellen wie Google Play, den Amazon Appstore und den Samsung Galaxy Store als vertrauenswürdig. Apps, die von nicht vertrauenswürdigen Quellen installiert worden sind, gelten als Sideloading-App.
Scannen von URLs in SMS-Textnachrichten auf iOS-Geräten	CylancePROTECT Mobile kann Benutzer vor potenziell schädlichen URLs in SMS-Textnachrichten warnen. Neu eingehende Textnachrichten von bekannten Kontakten werden automatisch als sicher angesehen. Nur Nachrichten von unbekannten Absendern werden gescannt und bewertet. Wenn ein Benutzer eine SMS-Textnachricht mit einer URL erhält, sendet die CylancePROTECT Mobile-App die gesamte Nachricht in Echtzeit an die CylancePROTECT-Cloud-Dienste. Die CylancePROTECT-Dienste nutzen erweiterte Maschinenlernfunktionen und gesammeltes Wissen aus Bedrohungserkennungs-Feeds, um eine sofortige Bewertung der Sicherheit der Nachricht zu ermöglichen. Wenn eine unsichere URL in einer Textnachricht erkannt wird, wird die Nachricht per Filter in den Spam-Ordner verschoben. Um die Privatsphäre der Benutzer zu schützen, werden nur Nachrichten ausgewertet, die URLs enthalten. Es werden keine weiteren Metadaten oder Benutzer-IDs erfasst oder gespeichert.
Scannen von URLs in SMS-Textnachrichten auf Android-Geräten	CylancePROTECT Mobile kann Benutzer vor potenziell schädlichen URLs in SMS-Textnachrichten warnen. Wenn ein Benutzer eine SMS-Textnachricht erhält, die eine URL enthält, wird die unveränderte URL in Echtzeit an die CylancePROTECT-Cloud-Dienste gesendet. Das Scannen von SMS ist auf die Standard-SMS-App auf dem Gerät beschränkt. Neu eingehende Textnachrichten von bekannten Kontakten und unbekannten Absendern werden gescannt und bewertet. Die CylancePROTECT-Dienste nutzen erweiterte Maschinenlernfunktionen und gesammeltes Wissen aus Bedrohungserkennungs-Feeds, um eine sofortige Bewertung der Sicherheit der URL zu ermöglichen. Wenn eine URL als unsicher eingestuft wird, warnt die CylancePROTECT Mobile-App den Benutzer, stellt Details bereit und leitet den Benutzer an, die Textnachricht zu löschen. Um die Privatsphäre der Benutzer zu schützen, werden nur Nachrichten ausgewertet, die URLs enthalten. Es werden keine weiteren Metadaten oder Benutzer-IDs erfasst oder gespeichert.

Funktion	Beschreibung
Prüfungen auf unsichere Netzwerk und unsichere Wi-Fi-Verbindungen	CylancePROTECT Mobile schützt vor den folgenden Netzwerkbedrohungen: • Unsichere Netzwerkverbindungen: Auf iOS- und Android-Geräten versucht die CylancePROTECT Mobile-App in regelmäßigen Abständen, eine Verbindung zu den CylancePROTECT-Cloud-Diensten herzustellen. Wenn die Verbindung nicht erfolgreich hergestellt werden kann, geht CylancePROTECT Mobile davon aus, dass das Netzwerk nicht sicher ist. • Unsichere Wi-Fi-Zugriffspunkte: Auf Android-Geräten überprüft die CylancePROTECT Mobile-App regelmäßig die Eigenschaften des aktuellen Wi-Fi-Zugriffspunkts, um festzustellen, ob dieser sicher ist. Sie können konfigurieren, welche Wi-Fi-Zugriffsalgorithmen in Ihrem Unternehmen als sicher bzw. unsicher gelten. Wenn die CylancePROTECT Mobile-App ein unsicheres Netzwerk oder einen unsicheren Wi-Fi-Zugriffspunkt erkennt, wird dies in der App und in der Verwaltungskonsole gemeldet.
Gerätesicherheitsprüfunge	Die CylancePROTECT Mobile-App überprüft bestimmte Gerätebedingungen und Sicherheitseinstellungen und benachrichtigt den Benutzer über potenzielle Schwachstellen in Bezug auf Cyberbedrohungen. Die App prüft Folgendes: • Ob der Entwicklermodus aktiviert ist (nur Android) • Ob die Festplattenverschlüsselung aktiviert ist (nur Android) • Ob eine Bildschirmsperre aktiviert ist (z. B. ein Kennwort oder ein Fingerabdruck) • Ob auf dem Gerät ein Rooting oder Jailbreak durchgeführt worden ist • Ob auf dem Gerät eine Betriebssystemversion ausgeführt wird, die Sie nicht unterstützen möchten • Ob Sie das Gerätemodell nicht unterstützen möchten Wenn die App eine Schwachstelle erkennt, zeigt sie die potenzielle Risikostufe an und gibt dem Benutzer Anweisungen zur Behebung des Problems.

Funktion	Beschreibung
Nachweisprüfungen	Die CylancePROTECT-Cloud-Dienste führen regelmäßig Nachweisprüfungen durch, um die Integrität und Sicherheit der CylancePROTECT Mobile-App auf dem Gerät jedes Benutzers zu überprüfen. Auf Android-Geräten verwenden die CylancePROTECT-Clouddienste den Play Integrity-Nachweis, den SafetyNet- und den Hardwarezertifikat-Nachweis, um die CylancePROTECT Mobile-App zu validieren. Der Play Integrity-Nachweis ersetzt den SafetyNet-Nachweis. Ältere Versionen der App unterstützen weiterhin den SafetyNet-Nachweis, bis Google den Support abstellt. Nachweisprüfungen werden täglich durchgeführt. Sie können auch eine Sicherheitspatch-Mindeststufe auf Geräten erzwingen. Wenn die App erkennt, dass das Gerät nicht die erforderliche Patch-Stufe erfüllt, kann sie den Benutzer darauf hinweisen, nach Updates zu suchen. Auf iOS-Geräten prüfen die CylancePROTECT-Cloud-Dienste die Integrität der App mithilfe des Apple DeviceCheck-Frameworks. Integritätsprüfungen werden täglich durchgeführt. Auf Samsung-Geräten können die CylancePROTECT Cloud-Dienste die Integrität der Geräte auch in regelmäßigen Abständen mithilfe von Samsung Knox Enhanced Attestation validieren. Knox Enhanced Attestation arbeitet hardwarebasiert und kann Gerätemanipulationen, Rooting, OEM-Entsperrung und Fälschung von IMEI- oder Seriennummern sowie die Durchführung von App-Zustandsprüfungen erkennen. Wenn ein Nachweisfehler auftritt, können Administratoren entsprechende Details in der Verwaltungskonsole anzeigen.
Integration in MDM-Lösungen	Sie können Cylance Endpoint Security mit Microsoft Intune verbinden, um Cylance Endpoint Security die Meldung einer Geräterisikostufe an Intune zu ermöglichen. Die Geräterisikostufe wird auf der Grundlage der Erkennung mobiler Bedrohungen durch die CylancePROTECT Mobile-App auf von Intune-verwalteten Geräten berechnet. Intune kann Risikominderungsmaßnahmen auf Basis der Geräterisikostufe ausführen.
Benutzerfreundlichkeit der CylancePROTECT Mobile-App	Für jede Funktion, die Sie in der CylancePROTECT Mobile-App aktivieren möchten, können Sie festlegen, ob Benutzer durch Gerätebenachrichtigungen oder E-Mail-Nachrichten über Bedrohungen informiert werden, oder keine Benachrichtigungen erhalten (Benutzer können Bedrohungswarnungen in der CylancePROTECT Mobile-App anzeigen). Die CylancePROTECT Mobile-App für Android Version 2.3.0.1640 und höher benachrichtigt den Benutzer, wenn eine neue Version der App in Google Play verfügbar ist. Nach 30 Tagen lädt die App das Update automatisch herunter und fordert Sie auf, das Update abzuschließen und die App neu zu starten. Nach 60 Tagen kann der Benutzer die App erst dann verwenden, wenn er auf die Aktualisierungsaufforderung reagiert. Die CylancePROTECT Mobile-App für iOS unterstützt automatische Updates aus dem App Store.

Architektur: CylancePROTECT Mobile



Element	Beschreibung
CylancePROTECT-Cloud-Dienste	Die Verwaltungskonsole und die CylancePROTECT Mobile-App auf den Geräten der Benutzer verwenden eine sichere Verbindung zur Kommunikation mit den CylancePROTECT-Cloud-Diensten, die für die Erstellung und Konfiguration von Benutzerkonten, die Anwendung von CylancePROTECT Mobile-Funktionen und -Einstellungen auf Geräten und die Verarbeitung von Ereignissen und Warnungen in Echtzeit verantwortlich sind. Die CylancePROTECT-Dienste nutzen KI und maschinelles Lernen, um festzustellen, ob Software und Websites potenziell schädlich sind und eine Bedrohung für die Sicherheit eines Geräts darstellen. Diese KI-Engine ist eine Kernkomponente verschiedener CylancePROTECT Mobile-Funktionen, darunter Malware-Erkennung, SMS-Nachrichtenscans, und Netzwerksicherheitsvalidierung. Im Kern ermöglicht die KI-Engine eine aggressive und proaktive Sicherheitsstrategie, bei der schädliche Software und Websites identifiziert werden, bevor sie sich auf die Infrastruktur oder die Gerätebenutzer Ihres Unternehmens auswirken können.
Verwaltungskonsole	Mit der Cloud-basierten Verwaltungskonsole können Sie mobile Geräte verwalten, CylancePROTECT Mobile-Funktionen konfigurieren und verwalten sowie den Gerätestatus und die von der CylancePROTECT Mobile-App erkannten mobilen Warnungen anzeigen.
BlackBerry Connectivity Node	BlackBerry Connectivity Node ist eine optionale Komponente, mit der Cylance Endpoint Security CylancePROTECT Mobile-Benutzer und -Gruppen mit Ihrem lokalen Microsoft Active Directory oder LDAP-Verzeichnis synchronisieren kann. Cylance Endpoint Security kann Benutzer und Gruppen mit Entra Active Directory ohne Verwendung von BlackBerry Connectivity Node synchronisieren.

Element	Beschreibung
Geräte mit der CylancePROTECT Mobile-App	Die CylancePROTECT Mobile-App, die auf iOS-, Android- und Chrome OS-Geräten installiert ist, scannt das Gerät in regelmäßigen Abständen und überprüft die Geräteeinstellungen und -bedingungen, um Bedrohungen zu identifizieren. Wenn die App eine Bedrohung erkennt, kann der Benutzer entsprechende Details in der App anzeigen. Wenn möglich, gibt die App dem Benutzer Anweisungen zum Beseitigen der Bedrohung und leitet ihn zu den Geräteeinstellungen, wo das Problem behoben werden kann.
MDM-Lösung	Sie können optional Cylance Endpoint Security mit Microsoft Intune verbinden, um Cylance Endpoint Security die Meldung einer Geräterisikostufe an Microsoft Intune zu ermöglichen. Die Geräterisikostufe wird auf der Grundlage der Erkennung mobiler Bedrohungen durch die CylancePROTECT Mobile-App auf von Intune-verwalteten Geräten berechnet. Intune kann Risikominderungsmaßnahmen auf Basis der Geräterisikostufe ausführen.

Was ist CylanceOPTICS?

CylanceOPTICS ist eine Endpunkterkennungs- und Reaktionslösung, die forensische Daten von Geräten sammelt und analysiert, um Bedrohungen zu identifizieren und abzuwehren, bevor sie sich auf die Benutzer und Daten Ihres Unternehmens auswirken.

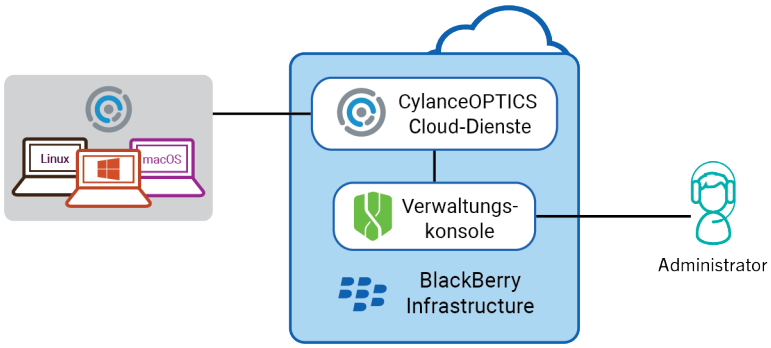
Sie aktivieren ein Windows-, macOS- oder Linux-Gerät für CylanceOPTICS, indem Sie den CylanceOPTICS-Agenten parallel zum CylancePROTECT Desktop-Agenten installieren. Der CylanceOPTICS-Agent stellt Sensoren auf verschiedenen Ebenen und Subsystemen im Betriebssystem bereit, um verschiedene Datensätze zu überwachen und zu erfassen, die in der CylanceOPTICS-Cloud-Datenbank aggregiert und gespeichert werden. Sie können CylanceOPTICS-Daten verwenden, um automatisierte Reaktionen auf gerätebasierte Bedrohungen zu erkennen, zu untersuchen, zu diagnostizieren und zu konfigurieren.

Wichtige Funktionen von CylanceOPTICS

Funktion	Beschreibung
Analysieren der CylanceOPTICS-Daten	Sie können die Verwaltungskonsole verwenden, um die vom CylanceOPTICS-Agenten erfassten Gerätedaten abzufragen und Sicherheitsvorfälle zu untersuchen sowie Gefährdungsindikatoren zu ermitteln. Wenn CylanceOPTICS eine Datei als potenzielle Bedrohung identifiziert, können Sie die Datei zur weiteren Analyse vom Gerät abrufen. Mit InstaQuery können Sie eine Reihe von Geräten nach dem Vorhandensein eines bestimmten Typs von forensischen Artefakten abfragen und feststellen, wie häufig dieses Artefakt auftritt. Erweiterte Abfragen sind eine Weiterentwicklung von InstaQuery, die mithilfe der EQL-Syntax detailliertere Suchfunktionen bietet, um die Erkennung von Bedrohungen zu verbessern.
Visualisieren von CylanceOPTICS-Daten	Sie können die folgenden Visualisierungsfunktionen zur Unterstützung Ihrer forensischen Analyse verwenden: • Die InstaQuery-Facettenaufschlüsselung bietet eine interaktive visuelle Anzeige der verschiedenen Facetten, die an einer Abfrage beteiligt sind, sodass Sie deren relationale Pfade identifizieren und verfolgen können. • Fokusdaten ermöglichen Ihnen die Visualisierung und Analyse der Ereigniskette und der damit verbundenen Artefakte und Facetten dieser Ereignisse, die zum Auftreten von Malware oder einer anderen Sicherheitsbedrohung auf einem Gerät geführt haben.

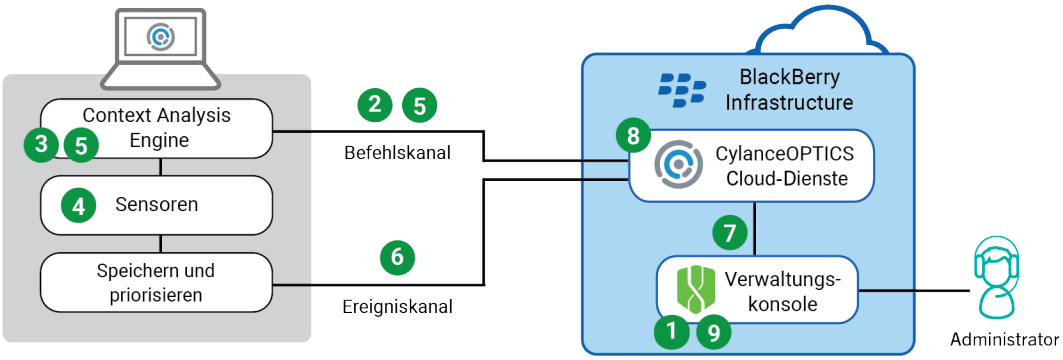
Funktion	Beschreibung
Ereignisse erkennen und darauf reagieren	CylanceOPTICS verwendet die Kontextanalyse-Engine (Context Analysis Engine, CAE), um auf Geräten auftretende Ereignisse nahezu in Echtzeit zu analysieren und korrelieren. Sie können CylanceOPTICS so konfigurieren, dass automatische Antwortaktionen durchgeführt werden, wenn die CAE bestimmte Artefakte von Interesse erkennt (z. B. Anzeigen einer Benachrichtigung oder Abmelden des aktuellen Benutzers), und eine zusätzliche Ebene zur Erkennung und Prävention von Bedrohungen geboten wird, um die Funktionen von CylancePROTECT Desktop zu ergänzen. Sie können die Erkennungsfunktionen von CylanceOPTICS an die Anforderungen Ihres Unternehmens anpassen. Sie können Erkennungsregelsätze mit der gewünschten Konfiguration von Regeln und Reaktionen erstellen, vorhandene Erkennungsregeln klonen und ändern oder eigene benutzerdefinierte Regeln erstellen. Außerdem haben Sie die Möglichkeit, Erkennungsausnahmen zu erstellen, um bestimmte Artefakte von der Erkennung auszuschließen.
Bereitstellen von Paketen zur Datenerfassung	Sie können die Funktion „Paket bereitstellen“ verwenden, um einen Prozess (z. B. ein Python-Skript) auf CylanceOPTICS-Geräten per Remote-Zugriff sicher auszuführen und die gewünschten Daten an einem bestimmten Standort zur weiteren Analyse zu erfassen und zu speichern. Sie können beispielsweise einen Prozess zur Erfassung von Browserdaten ausführen. Sie können die CylanceOPTICS-Datenerfassungspakete verwenden, die in der Verwaltungskonsole verfügbar sind, oder Sie können eigene erstellen.
Sperren von Geräten, um Bedrohungen zu isolieren	Sie können ein infiziertes oder potenziell infiziertes Gerät sperren und seine LAN- und Wi-Fi-Netzwerkfunktionen deaktivieren, um Befehls- und Steuerungsaktivitäten, die Datenextraktion und die laterale Bewegung von Malware zu stoppen. Es stehen verschiedene Sperroptionen zur Verfügung, um den Anforderungen Ihres Unternehmens gerecht zu werden.
Senden von Aktionen an Geräte	Sie können die Remote-Antwortfunktion verwenden, um Skripte sicher auszuführen und Befehle auf jedem CylanceOPTICS-fähigen Gerät mit einer vertrauten Befehlszeilenschnittstelle direkt von der Verwaltungskonsole aus auszuführen.

Architektur: CylanceOPTICS



Komponente	Beschreibung
CylanceOPTICS-Cloud-Dienste	Der CylanceOPTICS-Agent sendet die von ihm erfassten Gerätedaten an die CylanceOPTICS-Cloud-Dienste. Die Daten werden aggregiert und in der sicheren CylanceOPTICS-Cloud-Datenbank gespeichert. Die CylanceOPTICS-Datenanalysedienste bieten umfassende Interpretationen von Gerätedaten, auf die Sie über die Verwaltungskonsole zugreifen können. Bei Geräten bis zur CylanceOPTICS-Agent-Version 2.x wird die CylanceOPTICS-Datenbank lokal auf dem Gerät gespeichert. Ab Version 3.0 werden die Daten automatisch in regelmäßigen Zeitabständen aggregiert, gespeichert, komprimiert und an die CylanceOPTICS-Cloud-Datenbank gesendet.
Verwaltungskonsole	Mit der Cloud-basierten Verwaltungskonsole können Sie die auf Geräten installierten CylanceOPTICS-Agenten verwalten und CylanceOPTICS-Daten für die Untersuchung von Sicherheitsvorfällen abfragen. Sie können anpassen, welche Daten von CylanceOPTICS überwacht werden, wie es auf Ereignisse reagiert, und als Reaktion auf Bedrohungen Aktionen ausführen.
Geräte mit dem CylanceOPTICS-Agenten	Der CylanceOPTICS-Agent wird auf Windows-, macOS- und Linux-Geräten installiert. Der Agent stellt Sensoren für das Betriebssystem des Geräts zur Überwachung und Erfassung von Daten bereit, die zur Identifizierung von Bedrohungen und Auslösung automatisierter Reaktionen verwendet werden.

Datenfluss: Erkennung und Reaktion auf Ereignisse sowie Speicherung von Ereignisdaten (CylanceOPTICS 3.x und höher)



1. Ein Administrator verwendet die Verwaltungskonsole, um Erkennungsregeln zu konfigurieren und die Regeln einer Geräterichtlinie zuzuweisen.
2. Die CylanceOPTICS-Cloud-Dienste senden die Erkennungsregeln über eine sichere WebSocket-Verbindung an ein Gerät mit dem CylanceOPTICS-Agenten. Die Regeldaten enthalten auch die für das jeweilige Ereignis konfigurierten Reaktionen (z. B. Abmelden aller Benutzer, Aussetzen von Prozessen usw.).
3. Der CylanceOPTICS-Agent bezieht die Erkennungsregeln in die Context Analysis Engine (CAE) mit ein, die zur Analyse und Korrelation von Ereignissen verwendet wird.
4. Die CylanceOPTICS-Sensoren erkennen ein Ereignis.
5. Die CAE bestimmt, ob das Ereignis eine Erkennungsregel erfüllt. Falls ja, passiert Folgendes:
   - Wenn die Reaktion auf das Ereignis bereits für den CylanceOPTICS-Agenten konfiguriert ist, reagiert der Agent entsprechend.

- Wenn der Agent zusätzliche Daten für die Reaktion benötigt (z. B. ein Playbook-Paket erforderlich ist, das das Gerät noch nicht hat), sendet der Agent die Erkennungsdaten über eine sichere WebSocket-Verbindung an die CylanceOPTICS-Cloud-Dienste. Die CylanceOPTICS-Cloud-Dienste verarbeiten die Erkennung und stellen die Daten bereit, die der Agent zur Ausführung der Antwort benötigt.

6. Der Agent priorisiert die Ereignisdaten und sendet sie über einen dedizierten Ereigniskanal mithilfe einer sicheren TLS-Verbindung an die CylanceOPTICS-Cloud-Dienste. Die CylanceOPTICS-Cloud-Dienste empfangen und verarbeiten die Ereignisdaten und speichern sie in der sicheren CylanceOPTICS-Cloud-Datenbank.
7. Ein Administrator kann mithilfe der Verwaltungskonsole Nachweisdaten anfordern oder eine InstaQuery-, erweiterte Abfrage- oder Fokusansicht-Anforderung initiieren. Die Verwaltungskonsole interagiert mit den CylanceOPTICS-Cloud-Diensten mithilfe von HTTP über TLS.
8. Die CylanceOPTICS-Cloud-Dienste validieren und verarbeiten die Anforderung, rufen die angeforderten Daten aus der CylanceOPTICS-Cloud-Datenbank ab und senden die Daten an die Verwaltungskonsole zurück.
9. Die Erkennungsdaten, das Abfrageergebnis oder die Fokusdaten werden in der Verwaltungskonsole angezeigt.

Was ist CylanceGATEWAY ?

CylanceGATEWAY ist eine Cloud-native, KI-gestützte Zero-Trust-Netzwerkzugriffslösung (Zero Trust Network Access, ZTNA), die Ihren Benutzern Zugriff auf Ihre erweiterte Netzwerkumgebung ermöglicht und Ihr erweitertes Netzwerk vor Bedrohungen schützt. Die Unternehmen stehen heute vor großen Herausforderungen, da Cybersicherheitsbedrohungen immer komplexer und umfassender werden, während die Anzahl der vernetzten Unternehmensendpunkte und die Menge der Daten, die an die Cloud-Dienste gesendet und dort gespeichert werden, exponentiell zunehmen. CylanceGATEWAY bietet Netzwerksicherheit bei gleichzeitiger Verbesserung des Netzwerkerlebnisses für Endbenutzer. CylanceGATEWAY vertraut standardmäßig nichts und niemandem. Es wird davon ausgegangen, dass jeder Benutzer, jeder Endpunkt und jedes Netzwerk potenziell gefährlich ist und kein Benutzer auf etwas zugreifen kann, bis er beweist, wer er ist, dass sein Zugriff autorisiert ist, dass er nicht böswillig handelt und dass das lokale Netzwerk, mit dem er verbunden ist, nicht kompromittiert ist.

CylanceGATEWAY schützt die iOS-, Android-, Windows 10-, Windows 11 und macOS-Geräte der Benutzer, indem Sie Verbindungen zu Internetzielen blockieren können, mit denen die Geräte nicht kommunizieren sollen, selbst wenn das Gerät nicht mit Ihrem Netzwerk verbunden ist. BlackBerry pflegt eine ständig wachsende Liste unsicherer Internetziele, zu denen die Verbindungsaufnahme der Endpunkte blockiert werden kann. Wenn Ihr Unternehmen auch Benutzer daran hindern möchte, bestimmte Websites zu besuchen, die nicht Ihren Standards für die zulässige Nutzung entsprechen, können Sie Richtlinien erstellen, um zusätzliche Ziele festzulegen, auf die kein Benutzer zugreifen kann bzw. bestimmte Benutzer oder Gruppen nicht zugreifen können.

Wichtige Funktionen von CylanceGATEWAY

Funktion	Beschreibung
Arbeitsmodus	Benutzer können den Arbeitsmodus aktivieren und deaktivieren. Der Arbeitsmodus schützt Ihr Netzwerk und Ihre Geräte. Wenn dieser aktiviert ist, wird jeder Netzwerkzugriffsversuch anhand der ACL-Regeln (Access Control List, Zugriffssteuerungsliste) und der angegebenen Netzwerkschutzeinstellungen ausgewertet, die für Ihre Umgebung konfiguriert sind. Die Zugriffssteuerungsliste definiert zulässige und blockierte Ziele in privaten und öffentlichen Netzwerken. Wenn sie zulässig sind, wird der Netzwerkdatenverkehr über einen sicheren Tunnel zu den CylanceGATEWAY-Clouddiensten gesendet.
Unterstützung des Sicherheitsmodus für macOS und Windows	Sie können den Sicherheitsmodus für Benutzer aktivieren. Im Sicherheitsmodus blockiert CylanceGATEWAY den Zugriff von Anwendungen und Benutzern auf potenziell bösartige Ziele und erzwingt durch das Abfangen von DNS-Anforderungen eine Richtlinie für die zulässige Nutzung. Die CylanceGATEWAY-Clouddienste bewerten jede DNS-Abfrage anhand der konfigurierten ACL-Regeln und Netzwerkschutzeinstellungen (z. B. DNS-Tunneling und Zero-Day-Erkennung wie Domain Generation Algorithm [DGA], Phishing und Malware) und weisen den Agenten dann an, die Anfrage in Echtzeit zuzulassen oder zu blockieren. Wenn sie zulässig ist, wird die DNS-Anforderung normal über das Trägernetzwerk ausgeführt. Andernfalls setzt der CylanceGATEWAY-Agent die normale Reaktion außer Kraft, um den Zugriff zu verhindern. **Hinweis:** Wenn dieser Modus aktiviert ist, schützt er den gesamten DNS-Datenverkehr, der den CylanceGATEWAY-Tunnel nicht verwendet (z. B. Tunnelzugriff per App oder Split-Tunneling).

Funktion	Beschreibung
Agenten starten oder Arbeitsmodus auf macOS und Windows automatisch aktivieren	In der Gateway-Dienstrichtlinie können Sie erzwingen, dass der CylanceGATEWAY macOS Windows-Agent automatisch ausgeführt wird, wenn sich Benutzer anmelden, oder dass der Arbeitsmodus automatisch aktiviert wird, wenn der Agent startet. Ihre Richtlinieneinstellungen können die Einstellungen „CylanceGATEWAY bei Anmeldung starten“ und „Arbeitsmodus automatisch aktivieren“ im Agent außer Kraft setzen, aber Benutzer können den Arbeitsmodus nach dem Starten oder Schließen des Agenten manuell aktivieren und deaktivieren.
Integration in MDM-Lösungen	Sie können Cylance Endpoint Security mit BlackBerry UEM oder Microsoft Intune verbinden, damit Cylance Endpoint Security überprüfen kann, ob iOS- oder Android-Geräte von UEM oder Intune verwaltet werden. Sie können festlegen, ob Geräte von UEM oder Intune verwaltet werden müssen, bevor sie CylanceGATEWAY verwenden können. Weitere Informationen zu Netzwerkdiensten finden Sie unter Verbinden von Cylance Endpoint Security mit MDM-Lösungen, um zu überprüfen, ob Geräte verwaltet werden.
Tunnelzugriff per App auf macOS und iOS	Auf macOS- und iOS-Geräten unter Mobile Device Management (MDM) können Sie festlegen, welche Apps den CylanceGATEWAY-Arbeitsmodus-Tunnel verwenden dürfen. Sie können diese Option verwenden, um die geschäftliche Nutzung von persönlichen Geräten zu ermöglichen, ohne den Zugriff auf den Arbeitsmodus auf alle Anwendungen auf einem Gerät auszuweiten.
Per-App-Tunnelunterstützung auf Windows und Android	Auf Windows- und Android-Geräten können Sie festlegen oder einschränken, welche Apps den CylanceGATEWAY-Tunnel verwenden können.
Kontinuierliche Auswertung von Netzwerkzielen	BlackBerry verwendet maschinelles Lernen, IP-Reputation und Risikobewertung, um eine sich ständig weiterentwickelnde Liste schädlicher Internetziele zu verwalten. CylanceGATEWAY verhindert, dass Geräte eine Verbindung zu bekannten und unbekannten Phishing-Domains und zugehörigen IP- und FQDN-Zielen herstellen, sodass Ihr Unternehmen keine manuelle Zusammenstellung und Verwaltung einer eigenen Liste vornehmen muss.
Schutz vor Bedrohungen	CylanceGATEWAY nutzt maschinelles Lernen, um das Netzwerk Ihres Unternehmens kontinuierlich vor Bedrohungen zu schützen, indem Netzwerkverbindungen kontinuierlich auf potenzielle Bedrohungen überwacht werden. Wenn eine Anomalie erkannt wird, wird sie je nach der von Ihnen für Ihren Netzwerkschutz festgelegten Risikostufe anschließend blockiert oder es wird eine Warnung ausgegeben. • Endpunkte werden vor neu auftretenden Netzwerkbedrohungen und bekannten schädlichen Zielen geschützt. Identifizierte Anomalien (z. B. Zero Day, Phishing-Domains und Command and Control (C2) Beacons) • DNS-Tunneling-Anomalien werden anhand von CylanceGateway-Analysen des DNS-Datenverkehrs vom Client zum DNS-Server des Angreifers erkannt.
Bewerten der Risikostufe eines Netzwerkziels	Mithilfe der Verwaltungskonsole können Sie Risikostufen bewerten und die Kategorie und Unterkategorie von Netzwerkzielen identifizieren, so wie sie von den Cloud-Diensten von CylanceGATEWAY analysiert und festgelegt werden würden.

Funktion	Beschreibung
Unterstützung mehrerer privater Netzwerke	Sie können mehrere CylanceGATEWAY Connectors von einem Cylance Endpoint Security-Mandanten bereitstellen, um den Zugriff auf mehrere private Netzwerke (z. B. Segmente, Rechenzentren und VPCs) zu ermöglichen, die sich sowohl in einer lokalen als auch in einer Cloud-Umgebung befinden. Sie können die CylanceGATEWAY Connectors anzeigen, die jeder angegebenen Connector-Gruppe zugeordnet sind. Sie können maximal acht Connector-Gruppen erstellen und jeder Gruppe maximal acht CylanceGATEWAY Connector zuweisen.
Segmentierter privater Netzwerkzugriff	Sie können CylanceGATEWAY Connectors vor Ort und in privaten Cloud-Netzwerken installieren, um Netzwerkzugriff auf Remote-Geräte zu ermöglichen, ohne die Netzwerktopologie oder das Routing zu ändern und ohne Firewall-Lücken für eingehenden Datenverkehr zu öffnen. Der Zugriff über CylanceGATEWAY bietet eine starke Trennung. Nur die Teile des Netzwerks, die Sie auswählen, sind Endpunkten ausgesetzt, und Endpunkte werden nicht dem gesamten privaten Netzwerk ausgesetzt. Der CylanceGATEWAY Connector kann in einer AWS, vSphere, ESXi, Microsoft Entra ID oder Hyper-V Umgebung bereitgestellt werden.
Überwachen von Netzwerkzugriffen und Datenverkehrsmustern	Das CylanceGATEWAY-Dashboard in der Verwaltungskonsole zeigt mehrere Widgets an, die Verbindungen, Nutzungsmuster und Warnungen anzeigen, um Ihnen bei der Überwachung des Netzwerkverkehrs zu helfen.
Festlegen von Netzwerkschutzkonfigurationen	Auf dem Bildschirm „Netzwerkschutz“ können Sie festlegen, ob zulässige Netzwerkereignisse (z. B. Zielreputation und Signaturerkennungen), die unter der eingestellten minimalen Risikostufe liegen, auf dem Bildschirm „Netzwerkereignisse“ als Anomalien angezeigt werden. Wenn die zulässigen Ereignisse deaktiviert sind, werden sie als normaler zulässiger Datenverkehr angezeigt. Darüber hinaus können Sie die SIEM-Lösung oder die Syslog-Unterstützung so konfigurieren, dass nur gesperrte Ereignisse gesendet werden. Diese Funktionen ermöglichen eine detailliertere Kontrolle über Netzwerkschutz und SIEM-Lösung oder Syslog und können dazu beitragen, die Alarmmüdigkeit zu verringern.
Festlegen von Netzwerkschutzeinstellungen, die an die Ansicht „Warnungen“ gesendet werden sollen	Auf dem Bildschirm „Netzwerkschutz“ können Sie die Erkennungen (z. B. Zielreputation, Signaturerkennungen, DNS-Tunneling und Zero Day) festlegen, die Sie an die Ansicht „Warnungen“ senden möchten. Blockierte und zulässige ACL-Ereignisse werden nicht auf der Ansicht „Warnungen“ geteilt. Diese Funktion bietet eine detailliertere Steuerung der Warnungen, die in der Ansicht „Warnungen“ angezeigt werden.
Betriebssystemspezifische ACL-Regeln	Sie können ACL-Regeln erstellen und auf ein bestimmtes Betriebssystem anwenden. Sie können beispielsweise nur Desktop-Geräten Zugriff auf einige Ressourcen gewähren (macOS und Windows).
SaaS-Konfiguration mit nur einem Tastendruck	Sie können den Zugriff auf SaaS-Anwendungen mithilfe der Netzwerkdienste einfach konfigurieren. CylanceGATEWAY optimiert die Unterstützung von SaaS-Apps und ermöglicht eine schnellere Aktivierung der SaaS-App-Konnektivität in den ACL-Regeln, die Sie für Ihre Umgebung konfigurieren. Weitere Informationen zu Netzwerkdiensten finden Sie unter Definieren von Netzwerkdiensten.

Funktion	Beschreibung
Filtern von Inhalten	Die ACL-Regeln und die Netzwerkschutzeinstellungen, die Sie für Ihre Umgebung konfigurieren, filtern die Inhalte und Ziele, auf die Ihre Benutzer zugreifen können. Maschinelles Lernen und ACL-Regeln tragen dazu bei, dass die Benutzer und Geräte die akzeptablen Nutzungs- und regulatorischen Anforderungen Ihres Unternehmens erfüllen.
NAT-Detailberichte	Sie können Ereignisse basierend auf der Tunnel-IP-Adresse (BlackBerry-Quell-IP) filtern, um die Tunnel-IP-Adresse zu identifizieren, die von Benutzern für den Zugriff auf externe Ziele verwendet wird. Der CylanceGATEWAY Connector stellt zusätzliche Informationen über UDP- und TCP-Datenflüsse bereit, die durch den Tunnel zu Ihrem privaten Netzwerk fließen, nachdem Network Address Translation (NAT) angewendet wurde (z. B. Private NAT-Quell-IP und Privater Quellport). So können Sie die Quell-IP-Adresse und die Portnummer eines Ereignisses ermitteln, das als potenziell bösartig oder blockiert identifiziert wurde und Ihr privates Netzwerk durchquert.
Firewall für den Internetzugriff	CylanceGATEWAY schützt Geräte und Ihre privaten Netzwerke durch Filtern, Überwachen und Blockieren von Datenverkehr an potenziell verdächtige Ziele. CylanceGATEWAY komplettiert dies durch die Anwendung von ACL-Regeln, die für Ihre Umgebung und die von Ihnen festgelegten Netzwerkschutzeinstellungen konfiguriert sind. Weitere Informationen finden Sie in den folgenden Abschnitten: • Überwachen von Netzwerkverbindungen in der Dokumentation zur Administration. • Netzwerkzugriffssteuerung mithilfe von ACL-Regeln in der Dokumentation zur Einrichtung.
Unterstützung für Dienste mit IP-Pinning	Bei den meisten SaaS-Anwendungen kann mit Quell-IP-Pinning nur der Zugriff auf Verbindungen von einem bestimmten Bereich vertrauenswürdiger IP-Adressen beschränkt werden. Dadurch, dass die Benutzer Verbindungen nur über vertrauenswürdige Einstiegspunkte nutzen dürfen, können Unternehmen zusätzlich überprüfen, ob der Benutzer berechtigt ist, den Dienst zu nutzen. Ihr Unternehmen verwendet diese Methode möglicherweise bereits, um den Zugriff auf eine SaaS-Anwendung auf Verbindungen von IP-Adressen zu beschränken, die von Geräten verwendet werden, die mit dem Netzwerk Ihres Unternehmens verbunden sind. Für Benutzer, die ohne Verwendung von CylanceGATEWAY remote arbeiten, bedeutet dies, dass der gesamte Datenverkehr zwischen Remote-Geräten und einer SaaS-Anwendung über VPN zu Ihrem Netzwerk und dann zur SaaS-Anwendung geleitet werden muss. CylanceGATEWAY ermöglicht die Reservierung von CylanceGATEWAY-IP-Adressen, die Ihrem Unternehmen zugewiesen sind. Sie können diese IP-Adressen zusätzlich zu den IP-Adressen Ihres Unternehmens für das Quell-IP-Pinning verwenden, um die gleiche Sicherheitsstufe zu gewährleisten, ohne dass Remote-Benutzer mit dem VPN Ihres Unternehmens verbunden werden müssen.
Branchenführende Tunneltechnologie	CylanceGATEWAY bietet erweiterte Layer-3-Verschlüsselung für IP-Tunnel, die TCP-, UDP- und ICMP-, und Echtzeit-Datenverkehr mit geringer Latenz übertragen.

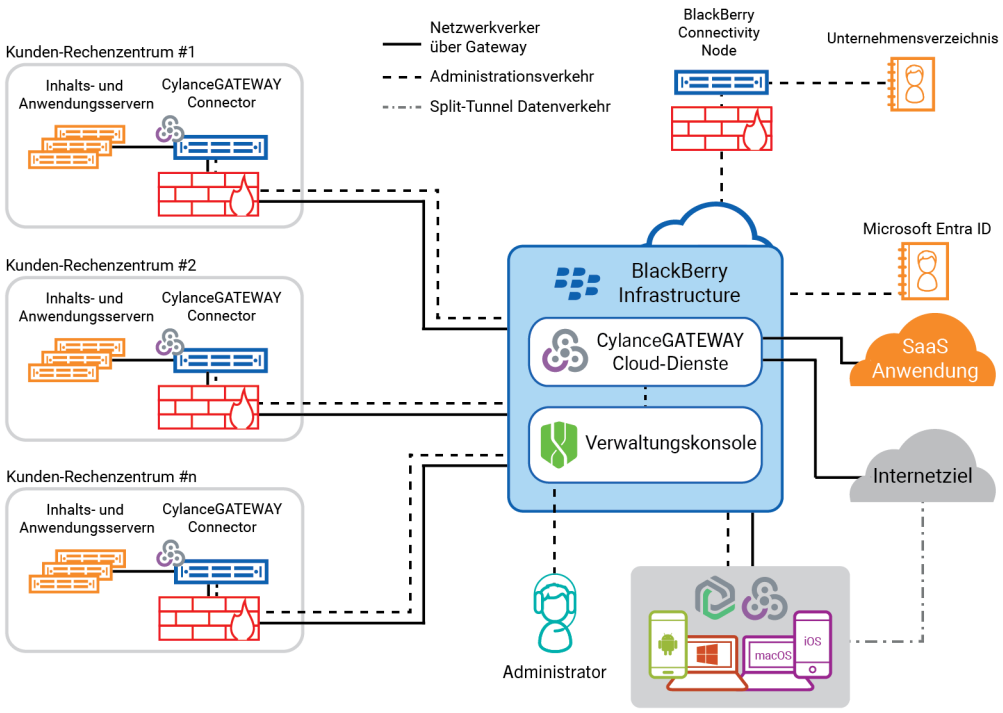
Funktion	Beschreibung
Android- und iOS-Unterstützung	Die CylancePROTECT Mobile-App sendet Datenverkehr durch den Tunnel an die CylanceGATEWAY-Clouddienste und stellt Benutzern Verbindungsstatistiken, Statusinformationen und die Möglichkeit zur Deaktivierung des Arbeitsmodus sowie zur Beendigung der Verwendung von CylanceGATEWAY für Verbindungen zur Verfügung.
Unterstützung für Windows 10, Windows 11 und macOS	Der CylanceGATEWAY-Agent, den Sie auf Geräten installieren, sendet Datenverkehr durch den Tunnel an die CylanceGATEWAY-Clouddienste und stellt Benutzern Verbindungsstatistiken, Statusinformationen und die Möglichkeit zur Deaktivierung des Arbeitsmodus sowie zur Beendigung der Verwendung von CylanceGATEWAY für Verbindungen zur Verfügung.
Split-Tunneling	Sie können Remote-Benutzern erlauben, sich ohne Tunneling per CylanceGATEWAY direkt über das Internet mit sicheren öffentlichen Websites zu verbinden. Wenn diese Option aktiviert ist, ermöglichen geteilte DNS-Abfragen die Durchführung von DNS-Abfragen für die Domänen, die in der Konfiguration Privates Netzwerk > DNS > Forward-Lookup-Zone aufgeführt sind, und über den Tunnel durchgeführt werden, in dem Netzwerkzugriffskontrollen angewendet werden. Alle anderen DNS-Suchen werden über Ihr lokales DNS durchgeführt. Wenn Sie den Sicherheitsmodus aktiviert haben, wird der DNS-Datenverkehr, der den Gateway-Tunnel nicht verwendet, durch den Sicherheitsmodus geschützt. Android- und 64-Bit-Chromebook-Geräte verwenden den Tunnel, in dem Netzwerkzugriffskontrollen angewendet werden.

Architektur: CylanceGATEWAY

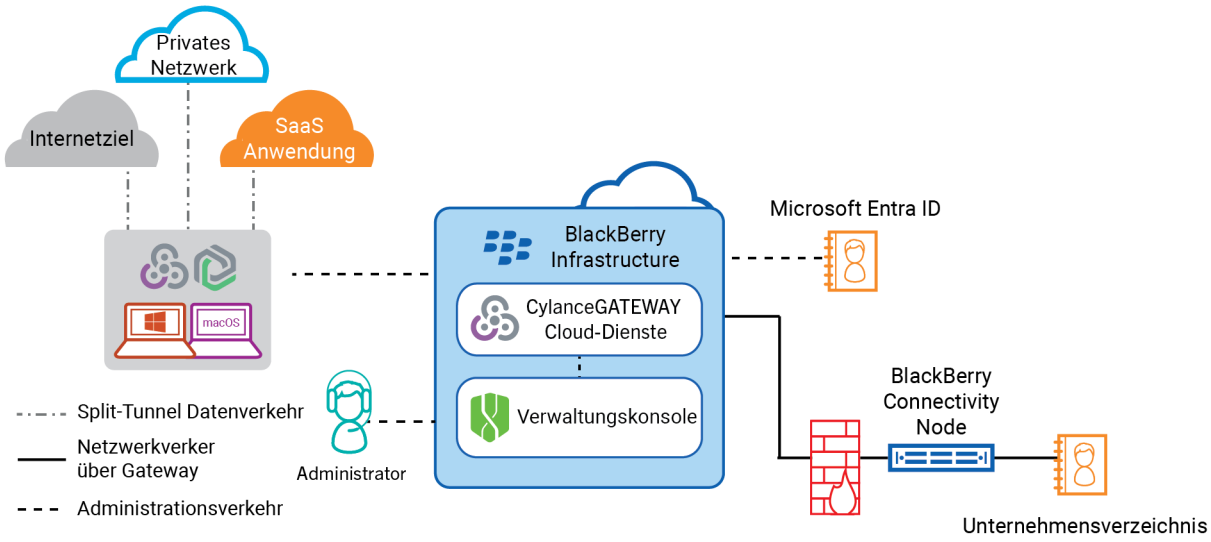
Die CylanceGATEWAY-Architektur wurde entwickelt, um Ihnen dabei zu helfen, die Geräte von Benutzern und Ihr erweitertes Netzwerk vor Bedrohungen zu schützen. Die folgenden Diagramme zeigen die Architektur von CylanceGATEWAY in den beiden Betriebsmodi.

- Arbeitsmodus: Der Arbeitsmodus erstellt einen sicheren Tunnel von Geräten über die CylanceGATEWAY-Clouddienste zu Netzwerkressourcen und schützt den gesamten Datenverkehr auf diesem Pfad.
- Sicherheitsmodus: Der Sicherheitsmodus erweitert die ACL-Regeln des Mandanten und den Endpunktschutz für macOS- und Windows-Geräte. Wenn diese Option aktiviert ist, wird der Sicherheitsmodus automatisch aktiviert, wenn der Arbeitsmodus deaktiviert ist. So wird sichergestellt, dass Geräte immer geschützt sind.

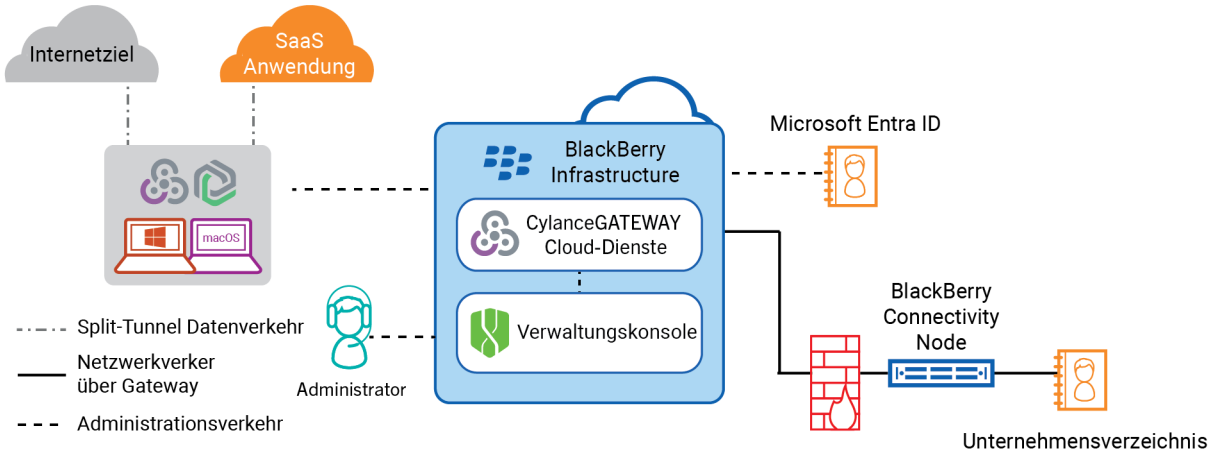
CylanceGATEWAY: Arbeitsmodus aktiviert



CylanceGATEWAY: Sicherheitsmodus für Benutzer im privaten Netzwerk aktiviert (z. B. Benutzer im Büro im Unternehmensnetzwerk)



CylanceGATEWAY: Sicherheitsmodus aktiviert für Benutzer in einem Remote-Netzwerk (z. B. auf Reisen)



Komponente	Beschreibung
CylanceGATEWAY-Cloud-Dienste	CylanceGATEWAY ist ein Cloud-basierter Dienst, der Zero-Trust-Netzwerkzugriff bietet, um Ihren Benutzern Zugriff auf Ihre erweiterte Netzwerkumgebung zu ermöglichen und Geräte und Ihr erweitertes Netzwerk vor Bedrohungen zu schützen. Die CylanceGATEWAY-Clouddienste nutzen maschinelles Lernen, um Netzwerkverbindungen kontinuierlich zu überwachen. Netzwerkanomalien werden erkannt, wenn ein CylanceGATEWAY-Benutzer versucht, eine Verbindung zu einem Ziel herzustellen, das verdächtig sein oder schädliche Inhalte enthalten könnte. Erkannte Anomalien können den Zugriff auf ein Ziel basierend auf dem für Ihre Umgebung konfigurierten Risikoschwellenwert blockieren.
Verwaltungskonsole	Die Cloud-basierte Verwaltungskonsole ermöglicht Ihnen die Konfiguration, Verwaltung und Überwachung von CylanceGATEWAY und der darüber vorgenommenen Verbindungen.
CylanceGATEWAY Connector	Der CylanceGATEWAY Connector ist eine optionale Komponente, die Sie hinter der Firewall und in privaten Netzwerken installieren können, um einen sicheren Tunnel zwischen den CylanceGATEWAY-Diensten und einem Ihrer privaten Netzwerke einzurichten. Der CylanceGATEWAY Connector ermöglicht Benutzern die Kommunikation mit Inhalts- und Anwendungsservern hinter der Firewall über CylanceGATEWAY statt über ein herkömmliches VPN.
BlackBerry Connectivity Node	BlackBerry Connectivity Node ist eine optionale Komponente, mit der Cylance Endpoint Security Benutzer und Gruppen mit Ihrem lokalen Microsoft Active Directory oder LDAP-Verzeichnis synchronisieren kann. Cylance Endpoint Security kann Benutzer und Gruppen mit Microsoft Entra ID ohne BlackBerry Connectivity Node synchronisieren.

Komponente	Beschreibung
Mobile Geräte mit der CylancePROTECT Mobile-App	CylanceGATEWAY unterstützt iOS- und Android-Geräte. Die auf Mobilgeräten installierte CylancePROTECT Mobile-App sendet Internetdatenverkehr über einen sicheren Tunnel an die CylanceGATEWAY-Clouddienste. Benutzer können den Arbeitsmodus aktivieren und deaktivieren, um anzugeben, ob der Datenverkehr den Tunnel zu den CylanceGATEWAY-Clouddiensten verwendet.
Desktop-Geräte mit dem CylanceGATEWAY-Agenten	CylanceGATEWAY unterstützt macOS- und Windows-10- und -11-Geräte. CylanceGATEWAY verfügt über zwei Betriebsmodi: • Im Arbeitsmodus sendet der CylanceGATEWAY-Agent Netzwerkdatenverkehr durch einen sicheren Tunnel an die CylanceGATEWAY-Clouddienste. Benutzer können den Arbeitsmodus aktivieren und deaktivieren, um anzugeben, ob der Datenverkehr den Tunnel verwendet. • Im Sicherheitsmodus blockiert CylanceGATEWAY den Zugriff von Anwendungen und Benutzern auf potenziell bösartige Ziele und erzwingt durch das Abfangen von DNS-Anforderungen eine Richtlinie für die zulässige Nutzung. Die CylanceGATEWAY-Cloud wertet jede DNS-Abfrage anhand der konfigurierten ACL-Regeln und Netzwerkschutzeinstellungen aus und weist dann den Agenten an, die Anforderung in Echtzeit zuzulassen oder zu blockieren. Wenn sie zulässig ist, wird die DNS-Anforderung normal über das Trägernetzwerk ausgeführt. Andernfalls setzt der CylanceGATEWAY-Agent die normale Reaktion außer Kraft, um den Zugriff zu verhindern. Wenn der Sicherheitsmodus aktiviert ist, können Benutzer, die sich im privaten Netzwerk befinden (z. B. im Büro), auf Ressourcen in Ihrem privaten Netzwerk zugreifen. Benutzer in Remote-Netzwerken haben keinen Zugriff auf Ressourcen in Ihrem privaten Netzwerk.
SaaS-Anwendungen	Software-as-a-Service-Anwendungen bieten Cloud-basierte Unternehmenssoftware, die Benutzern Anwendungen und Daten auf mehreren Geräten zur Verfügung stellt. Anwendungen und Daten befinden sich überwiegend auf Cloud-basierten Servern, die vom Anbieter verwaltet werden. Dies erleichtert die Bereitstellung und senkt die Kosten für die Infrastruktur vor Ort. Es sind jedoch Sicherheitsmaßnahmen erforderlich, die über Firewalls und andere umgebungsbasierte Sicherheitsmethoden hinausgehen. CylanceGATEWAY kann den Benutzerzugriff auf SaaS-Anwendungen sichern, ohne dass Datenverkehr durch das private Netzwerk Ihres Unternehmens geleitet werden muss, indem Quell-IP-Pinning aktiviert wird.
Internetziele	Zu öffentlichen Internetzielen gehören Websites, SaaS-Anwendungen und andere Objekte mit einer IP-Adresse, zu denen eine Client-App über das Internet eine Verbindung herstellen kann. BlackBerry führt eine ständig wachsende Liste von Zielen, die als schädlich bekannt sind. CylanceGATEWAY kann verhindern, dass Apps auf Geräten eine Verbindung zu auf der Liste enthaltenen Zielen herstellen. Wenn Sie Split-Tunneling aktivieren, kann der Datenverkehr zwischen Geräten und den von Ihnen angegebenen sicheren öffentlichen Websites direkt über das Internet anstatt über CylanceGATEWAY abgewickelt werden.

So sendet CylanceGATEWAY Daten im Arbeitsmodus

Wenn Ihre Benutzer versuchen, auf Ziele im privaten Netzwerk oder auf ein öffentliches Internetziel zuzugreifen, können sie nur dann auf diese zugreifen, wenn Sie dies durch die ACL-Regeln (Access Control List) ausdrücklich zugelassen haben. Jeder Netzwerkzugriffsversuch wird anhand der ACL-Regeln und der angegebenen Netzwerkschutzeinstellungen ausgewertet, die für Ihre Umgebung konfiguriert sind. Wenn eine ACL-Regel das Ziel blockiert, sperrt CylanceGATEWAY die Verbindung und leitet den Datenverkehr nicht weiter. Wenn Benutzer aufgrund einer ACL-Regel auf das private Netzwerk oder ein öffentliches Internetziel zugreifen können, wird die Verbindung alle fünf Minuten neu ausgewertet und die ACL-Regeln werden erneut angewendet. Wenn sich die Risikostufe eines Benutzers geändert hat oder die Zielreputation seit der Einrichtung des Zugriffsversuchs aktualisiert wurde, wird die Verbindung möglicherweise getrennt. Wenn eine ACL-Regel Benutzern den Zugriff auf ein Ziel ermöglicht, kann die Verbindung anschließend blockiert oder auf der Grundlage der identifizierten Anomalien und der Risikostufe, die für die Netzwerkschutzeinstellungen festgelegt wurde, eine Warnung ausgegeben werden.

- Wenn sich das Upload- oder Download-Volumen eines Benutzers geändert hat, weist CylanceGATEWAY auf das ungewöhnliche Datenverkehrsmuster hin, blockiert jedoch nicht den Datenverkehr des Benutzers.
- Wenn der Benutzer versucht, auf ein Ziel zuzugreifen, das sich auf der BlackBerry-Liste der unsicheren Internetziele befindet oder neuerdings als schädlich identifiziert wurde, und der Risikoschwellenwert für den Netzwerkschutz auf hoch gesetzt ist, wird der Zugriff des Benutzers blockiert.

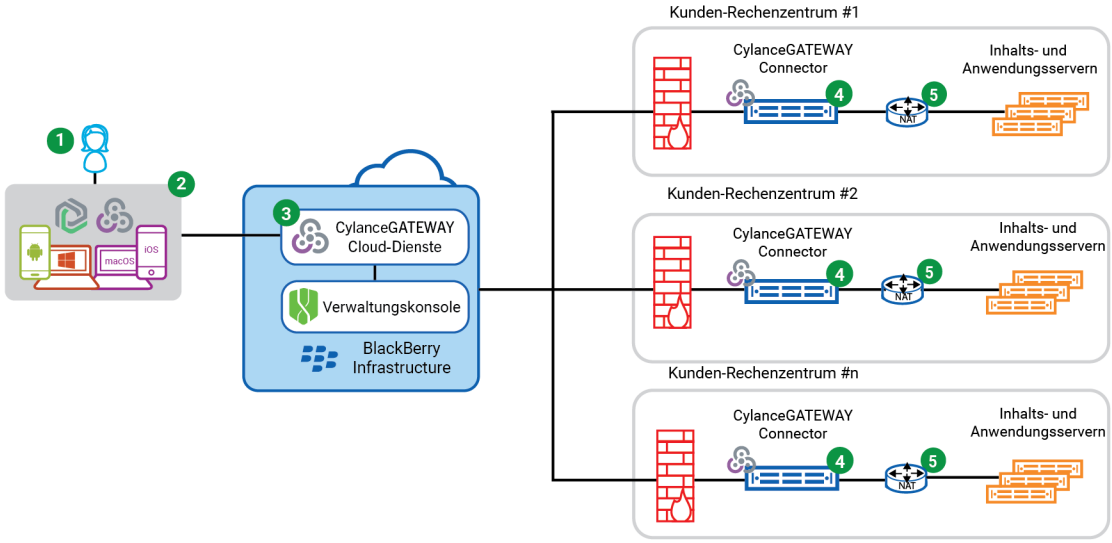
Wenn CylanceGATEWAY auf einem Gerät aktiv ist, leitet CylanceGATEWAY den Netzwerkdatenverkehr wie folgt weiter.

Ziel	Aktion
Zulässiges Ziel im privaten Netzwerk	Benutzer können nur dann auf Ziele in Ihrem privaten Netzwerk zugreifen, wenn sie ausdrücklich durch die Regeln der Zugriffssteuerungsliste (ACL) dazu berechtigt sind. ACL-Regeln bewerten jeden Netzwerkzugriffsversuch und ermöglichen den Zugriff auf das private Netzwerk, wenn eine Regelübereinstimmung gefunden wird. Alle Daten zwischen dem Gerät und Ihrem privaten Netzwerk werden mithilfe branchenführender Tunneltechnologie verschlüsselt und von der CylancePROTECT Mobile-App oder dem CylanceGATEWAY-Agent zur BlackBerry Infrastructure und dann von der BlackBerry Infrastructure zum hinter Ihrer Firewall installierten CylanceGATEWAY Connector durch sichere Tunnel geleitet.
Zulässiges Internetziel	Benutzer können nur dann eine Verbindung zu einem öffentlichen Internetziel herstellen, wenn sie ausdrücklich durch Ihre ACL-Regeln dazu berechtigt sind. ACL-Regeln bewerten jeden Netzwerkzugriffsversuch und ermöglichen den Zugriff auf das Ziel, wenn eine Regelübereinstimmung gefunden wird. Verbindungen zu öffentlichen Internetzielen werden über den sicheren Tunnel zwischen der CylancePROTECT Mobile-App oder dem CylanceGATEWAY-Agent und der BlackBerry Infrastructure geleitet und CylanceGATEWAY leitet dann den Datenverkehr an das Ziel weiter. Wenn Sie Split-Tunneling aktivieren, wird der Datenverkehr zu sicheren Internetzielen direkt an das Ziel und nicht über den Tunnel zu CylanceGATEWAY geleitet. Sie können beispielsweise den über CylanceGATEWAY geleiteten Datenverkehr reduzieren, indem Sie zulassen, dass der Datenverkehr zu sicheren öffentlichen Websites direkt zum Ziel geleitet wird.

Ziel	Aktion
Zulässige SaaS-App	Standardmäßig werden Verbindungen zu SaaS-Apps auf die gleiche Weise wie Verbindungen zu anderen Internetzielen geleitet. Wenn Sie Quell-IP-Pinning aktivieren, können Sie Ihren SaaS-App-Mandanten so konfigurieren, dass nur Verbindungen von den eigenen IP-Adressen Ihres Unternehmens und CylanceGATEWAY akzeptiert werden.
Blockiertes Ziel im privaten Netzwerk	Benutzer können nur dann auf Ziele in Ihrem privaten Netzwerk zugreifen, wenn sie ausdrücklich durch die ACL-Regeln dazu berechtigt sind. Wenn das Ziel nicht zulässig ist, blockiert CylanceGATEWAY die Verbindung und leitet den Datenverkehr nicht an CylanceGATEWAY Connector weiter. Wenn Benutzer versuchen, auf ein Ziel zuzugreifen, das durch eine ACL-Regel blockiert wird, wird der Versuch und die Ursache auf dem Warnmeldungsbildschirm im CylanceGATEWAY-Agenten des Benutzers angezeigt.
Blockiertes Internetziel	Wenn ein Ziel explizit von Ihren ACL-Regeln blockiert oder von BlackBerry als potenziell schädliches Ziel erfasst wird, blockiert CylanceGATEWAY die Verbindung. Wenn Benutzer versuchen, auf ein Ziel zuzugreifen, das durch eine ACL-Regel blockiert wird, werden der Versuch und die Ursache auf dem Warnungsbildschirm im CylanceGATEWAY-Agenten des Benutzers angezeigt.

Datenfluss: Zugreifen auf einen Anwendungs- oder Inhaltsserver in Ihrem privaten Netzwerk

Dieser Datenfluss beschreibt, wie über CylanceGATEWAY Daten zwischen Geräten und Servern in Ihren privaten Netzwerken übertragen werden.



Das obige Diagramm zeigt die folgende Reihenfolge.

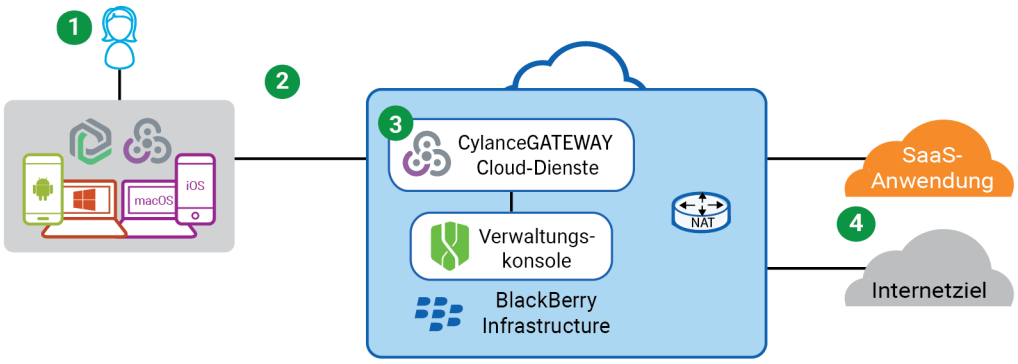
1. Der Benutzer aktiviert den Arbeitsmodus und öffnet eine App und versucht, auf eine Ressource in einem Ihrer privaten Netzwerke zuzugreifen.
2. Die CylancePROTECT Mobile-App oder der CylanceGATEWAY-Agent auf dem Gerät leitet die Verbindung über einen sicheren Tunnel zum CylanceGATEWAY in der BlackBerry Infrastructure.
3. CylanceGATEWAY führt die folgenden Aktionen aus:

a. Basierend auf den Regeln der Zugriffssteuerungsliste (ACL) wird festgelegt, ob der Benutzer Zugriff auf diesen Standort im privaten Netzwerk hat.
b. Wenn der Benutzer Zugriff hat, wird die Verbindung durch einen sicheren Tunnel zum CylanceGATEWAY Connector geleitet.

4. Der CylanceGATEWAY Connector leitet die Verbindung zu ihrem Ziel im privaten Netzwerk weiter.
5. Der CylanceGATEWAY Connector wendet NAT (Network Address Translation) auf Datenströme mit einem Ziel in Ihrem privaten Netzwerk an. Der Connector bietet zusätzliche Informationen zu UDP- und TCP-Flows, mit denen Sie die IP-Quelladresse und Portnummer eines blockierten oder als potenziell schädlich identifizierten Ereignisses identifizieren können. Sie können über das private Netzwerk nicht mit Remote-IT-Tools (z. B. Remote Desktop Connection) auf den CylanceGATEWAY Connector-Endpunkt zugreifen.

Datenfluss: Zugriff auf Cloud-basierte Anwendungen oder Internetziele

Dieser Datenfluss beschreibt, wie Daten zwischen Geräten und einer Cloud-basierten SaaS-Anwendung oder öffentlichen Internetzielen über CylanceGATEWAY übertragen werden.



Das obige Diagramm zeigt die folgende Reihenfolge.

1. Der Benutzer aktiviert den Arbeitsmodus, öffnet eine App und versucht, über das Internet auf eine Cloud-basierte Anwendung oder ein Ziel zuzugreifen.
2. Die CylancePROTECT Mobile-App oder der CylanceGATEWAY-Agent auf dem Gerät sendet die verschlüsselten Daten über einen sicheren Tunnel an CylanceGATEWAY in der BlackBerry Infrastructure.
3. CylanceGATEWAY führt die folgenden Aktionen aus:
   a. Basierend auf den Regeln der Zugriffssteuerungsliste (ACL) wird festgelegt, ob der Benutzer Zugriff auf diesen Standort hat.
   b. Wenn der Benutzer Zugriff hat, werden die Daten an die SaaS-Anwendung gesendet oder der Zugriff auf das Internetziel ermöglicht.
   c. Wendet Network Address Translation (NAT) auf Datenströme an, die auf SaaS-Apps und Internetziele zugreifen, indem die IP-Quelladresse ersetzt wird.
4. Wenn Quell-IP-Pinning aktiviert ist, überprüft die SaaS-Anwendung, ob die Verbindung von einer IP-Adresse stammt, die mit Ihrem CylanceGATEWAY-Mandanten verknüpft ist, bevor der Zugriff zugelassen wird.

So sendet CylanceGATEWAY Daten im Sicherheitsmodus

Wenn Ihre Benutzer versuchen, auf ein öffentliches Internetziel zuzugreifen, können sie nur dann auf dieses zugreifen, wenn Sie es durch die ACL-Regeln (Access Control List) ausdrücklich zugelassen haben. Wenn der Sicherheitsmodus aktiviert ist, blockiert CylanceGATEWAY den Zugriff von Benutzern auf potenziell

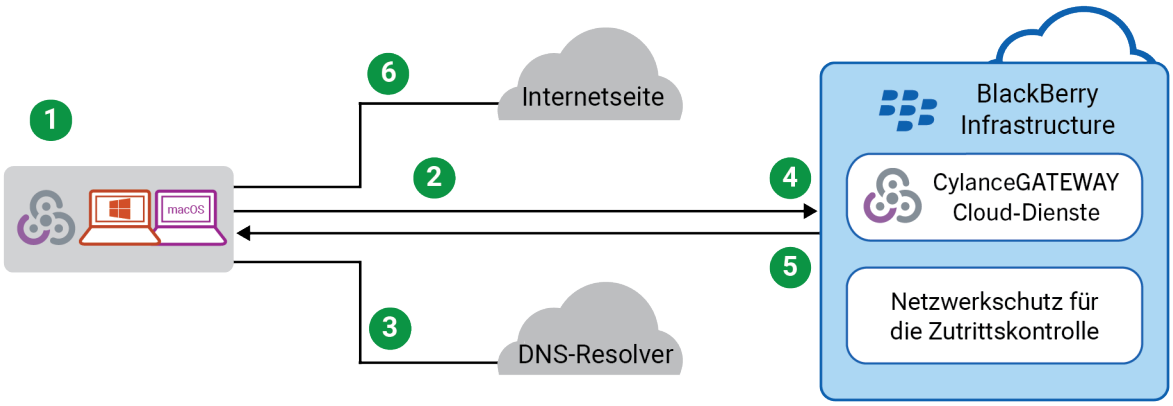
bösartige Ziele und erzwingt durch das Abfangen von DNS-Anforderungen eine Richtlinie für die zulässige Nutzung. Die CylanceGATEWAY-Clouddienste werten jede DNS-Abfrage anhand der konfigurierten ACL-Regeln und Netzwerkschutzeinstellungen aus und weisen dann den Agenten an, die Anforderung in Echtzeit zuzulassen oder zu blockieren. Wenn die ACL-Regel ein Ziel blockiert, verhindert CylanceGATEWAY den Zugriff. Wenn es zulässig ist, kann die Netzwerk-DNS-Abfrage über das Trägernetzwerk durchgeführt werden.

Wenn der Sicherheitsmodus auf einem macOS- oder Windows-Gerät aktiviert ist, sendet CylanceGATEWAY den Netzwerkdatenverkehr wie folgt.

Ziel	Aktion
Zulässiges Internetziel	Benutzer können nur dann auf ein öffentliches Internetziel zugreifen, wenn es ausdrücklich durch Ihre ACL-Regeln zulässig ist. ACL-Regeln bewerten jeden Netzwerkzugriffsversuch und ermöglichen den Zugriff auf das Ziel, wenn eine Regelübereinstimmung gefunden wird. Wenn Sie den Sicherheitsmodus aktivieren, wird der Datenverkehr zu sicheren Internetzielen über das Trägernetzwerk zum Ziel geleitet, anstatt durch den CylanceGATEWAY-Tunnel. Wenn Sie Split-Tunneling aktivieren, wird der Datenverkehr zu sicheren Internetzielen über das Trägernetzwerk zum Ziel geleitet und ist durch den Sicherheitsmodus geschützt. Dadurch wird der über CylanceGATEWAY geleitete Datenverkehr reduziert, da Sie zulassen, dass der Datenverkehr zu sicheren öffentlichen Websites direkt zum Ziel geleitet wird.
Blockiertes Internetziel	Wenn ein Ziel explizit von Ihren ACL-Regeln blockiert oder von BlackBerry als potenziell schädliches Ziel erfasst wird, blockiert CylanceGATEWAY die DNS-Abfrage. Wenn Benutzer versuchen, auf ein Ziel zuzugreifen, das durch eine ACL-Regel blockiert wird, werden der Versuch und die Ursache auf dem Warnungsbildschirm im CylanceGATEWAY-Agenten des Benutzers angezeigt.

Datenfluss: Zugreifen auf Inhalte, Anwendungen und öffentliche Internetziele im Sicherheitsmodus

Dieser Datenfluss beschreibt, wie Daten im Sicherheitsmodus zwischen Geräten und einem öffentlichen Internetziel übertragen werden. Im Sicherheitsmodus blockiert CylanceGATEWAY den Zugriff von Anwendungen und Benutzern auf potenziell bösartige Ziele und erzwingt durch das Abfangen von DNS-Anforderungen eine Richtlinie für die zulässige Nutzung. Die CylanceGATEWAY-Clouddienste werten jede DNS-Abfrage anhand der konfigurierten ACL-Regeln und Netzwerkschutzeinstellungen aus und weisen dann den Agenten an, die Anforderung in Echtzeit zuzulassen oder zu blockieren. Wenn sie zulässig ist, wird die DNS-Anforderung normal über das Trägernetzwerk ausgeführt. Andernfalls setzt der CylanceGATEWAY-Agent die normale Reaktion außer Kraft und verhindert den Zugriff.



Das obige Diagramm zeigt die folgende Reihenfolge.

1. Der CylanceGATEWAY-Agent hat den Sicherheitsmodus aktiviert und der Benutzer versucht, auf ein Internetziel zuzugreifen.
2. Der CylanceGATEWAY-Agent fängt die DNS-Anforderung ab, die vom Gerät gestellt wird, und fragt die CylanceGATEWAY-Clouddienste mit Informationen aus dieser Anforderung ab.
3. Der Agent stellt die DNS-Anforderung an den ursprünglichen DNS-Server.
4. Die CylanceGATEWAY-Clouddienste werten jede Abfrage anhand der konfigurierten ACL-Regeln und Netzwerkschutzeinstellungen aus und weisen dann den Agenten an, die Anforderung zuzulassen oder zu blockieren.
5. Wenn der Zugriff zulässig ist, leitet der Agent die Antwort des ursprünglichen DNS-Servers als Antwort auf die ursprüngliche DNS-Anforderung zurück. Andernfalls fügt der Agent eine DNS-Antwort ein, die den Zugriff blockiert.
6. Der Agent verwendet die Ergebnisse einer zulässigen DNS-Anforderung, um auf ein Internetziel zuzugreifen.

Was ist CylanceAVERT ?

CylanceAVERT ist eine Lösung zum Schutz von Informationen, die den Verlust sensibler regulatorischer und organisatorischer Informationen über externe Quellen erkennt und verhindert. CylanceAVERT kann vertrauliche Unternehmensinformationen erkennen, kategorisieren und inventarisieren und Bedrohungserkennung bereitstellen, um nicht autorisierte Exfiltrationsereignisse zu verhindern. Neben der Bereitstellung eines Bestands an vertraulichen Dateien und der Verwaltung von Bedrohungsereignissen scannt CylanceAVERT Dateien, die auf ein USB-Gerät kopiert, auf einen Browser-Speicherort oder ein Netzlaufwerk hochgeladen oder im Text oder in den Anhängen von E-Mail-Nachrichten gespeichert wurden, und eine Korrekturmaßnahme empfehlen.

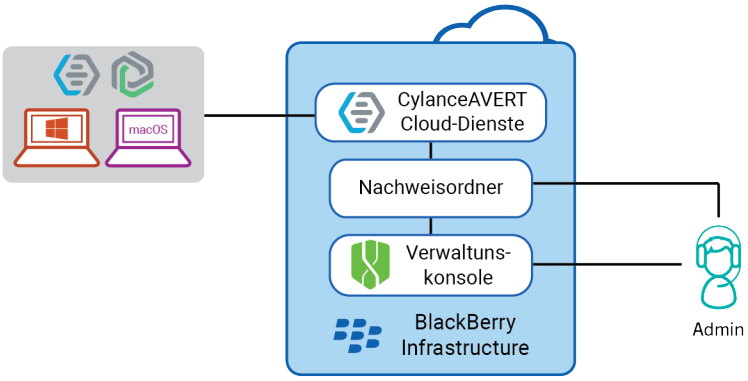
Wenn ein Benutzer versucht, sensible Daten über ein USB-Gerät, eine Browser-Domäne oder in einer E-Mail-Nachricht hochzuladen, scannt CylanceAVERT den Inhalt und ermittelt anhand der Datenschutzrichtlinien, ob er als vertraulich eingestuft werden muss. Der Benutzer erhält eine Warnung, wenn die Richtlinie verletzt wurde, und die konfigurierte Korrekturmaßnahme wird angewendet.

Wichtige Funktionen von CylanceAVERT

Funktion	Beschreibung
Scannen sensibler Daten	CylanceAVERT kann auf USB-Laufwerke, Internetbrowser und als E-Mail-Anhänge hochgeladene Dateien sowie den Inhalt einer E-Mail-Nachricht auf Unternehmensdaten scannen, die der Administrator in den Informationsschutzrichtlinien als vertraulich definiert hat. Falls Daten-Exfiltrationsereignisse vorliegen sollten, wird eine E-Mail-Benachrichtigung gesendet.
Richtlinien zum Informationsschutz	Sie können die Bedingungen angeben, die zum Auslösen einer Richtlinienverletzung erfüllt sein müssen, die zulässigen Domänen für die Richtlinie und die Aktionen, die bei einer Richtlinienverletzung ausgeführt werden sollen. Weitere Informationen finden Sie unter Verwalten von Richtlinien zum Schutz von Informationen im Einrichtungshandbuch für Cylance Endpoint Security.
CylanceAVERT-Ereignisse	Sie können Richtlinien zum Schutz von Informationen erstellen, um die Daten und Bedingungen anzugeben, die erfüllt werden müssen, um einen Richtlinienverstoß auszulösen. Zudem können Sie die Standorte festlegen, für die die Richtlinie gilt, die zu überwachenden Aktivitäten und die zu ergreifenden Abhilfemaßnahmen, wenn eine Richtlinie verletzt wurde. Weitere Informationen finden Sie unter CylanceAVERT-Ereignisse im Administratorhandbuch für Cylance Endpoint Security.

Funktion	Beschreibung
Informationsschutz-Einstellungen	Mithilfe der Einstellungen zum Informationsschutz können Sie sensible Daten konfigurieren, die überwacht werden sollen. Hierzu fügen Sie Vorlagen und Datentypen hinzu, die in der Informationsschutzrichtlinie verwendet werden sollen. Administratoren können auch die zulässigen und vertrauenswürdigen Browser- und E-Mail-Domänen definieren, die Nachweise verwalten, die für Daten-Exfiltrationsereignisse erfasst werden, und festlegen, wie lange die Nachweise verfügbar sein sollen. An die angegebenen E-Mail-Adressen können auch Benachrichtigungen über Daten-Exfiltrationsereignisse gesendet werden. Weitere Informationen finden Sie unter Definieren vertraulicher Inhalte mithilfe von Einstellungen zum Schutz von Informationen im Einrichtungshandbuch für Cylance Endpoint Security.
Dateibestand	Der CylanceAVERT-Dateibestand erstellt einen Datensatz aller sensiblen Dateien in einem Unternehmen über einen Datei-Suchprozess. Weitere Informationen finden Sie unter Verwenden des Dateibestands zum Identifizieren sensibler Dateien im Administratorhandbuch für Cylance Endpoint Security
Nachweisordner	Mithilfe des Nachweisordners können Sie die Details der Dateien anzeigen, die an Exfiltrationsereignissen beteiligt waren, und die Dateien zu Prüfzwecken in ihren lokalen Speicher herunterladen. Weitere Informationen finden Sie unter Verwenden des Nachweisordners zum Anzeigen von Details zu Exfiltrationsereignissen im Administratorhandbuch für Cylance Endpoint Security

Architektur: CylanceAVERT



Element	Beschreibung
CylanceAVERT	CylanceAVERT verhindert den Verlust sensibler Daten durch Exfiltration über E-Mail-Nachrichten und -Anhänge, Browser-Uploads und USB-Geräte.
Nachweisordner	Der Nachweisordner ist ein privater Dateispeicherbereich, in dem Dateien gespeichert werden, die an nicht autorisierten Exfiltrationsereignissen beteiligt sind, um von Administratoren weiter geprüft zu werden.

Element	Beschreibung
Verwaltungskonsole	Über die Cloud-basierte Verwaltungskonsole können Sie die zu überwachenden und zu schützenden sensiblen Unternehmensdaten definieren, Benutzerrichtlinien verwalten, um die Bedingungen festzulegen, die erfüllt sein müssen, um ein Exfiltrationsereignis auszulösen, die sensiblen Dateien in Ihrem Unternehmen anzeigen und verschiedene bedrohungsbezogene Ereignisse zur Risikobewertung und -behebung anzeigen.
Geräte mit CylanceAVERT und CylancePROTECT	CylancePROTECT Desktop muss auf dem Endpunkt installiert sein, um die Funktionalität von CylanceAVERT nutzen zu können. CylanceAVERT unterstützt Windows 10 und 11.

Rechtliche Hinweise

Patente, sofern zutreffend, zu finden unter: www.blackberry.com/patents.

Dieses Dokument und alle Dokumente, die per Verweis in dieses Dokument mit einbezogen werden, z. B. alle über die BlackBerry-Webseite erhältlichen Dokumente, werden ohne Mängelgewähr und je nach Verfügbarkeit bereitgestellt. Die entsprechenden Dokumente werden ohne ausdrückliche Billigung, Gewährleistung oder Garantie seitens BlackBerry Limited und seinen angegliederten Unternehmen („BlackBerry“) bereitgestellt. BlackBerry übernimmt keine Verantwortung für eventuelle typografische, technische oder anderweitige Ungenauigkeiten sowie für Fehler und Auslassungen in den genannten Dokumenten. Die BlackBerry-Technologie ist in dieser Dokumentation teilweise in verallgemeinerter Form beschrieben, um das Eigentum und die vertraulichen Informationen und/oder Geschäftsgeheimnisse von BlackBerry zu schützen. BlackBerry behält sich das Recht vor, die in diesem Dokument enthaltenen Informationen von Zeit zu Zeit zu ändern. BlackBerry ist jedoch nicht verpflichtet, die Benutzer über diese Änderungen, Updates, Verbesserungen oder Zusätze rechtzeitig bzw. überhaupt in Kenntnis zu setzen.

Diese Dokumentation enthält möglicherweise Verweise auf Informationsquellen, Hardware oder Software, Produkte oder Dienste, einschließlich Komponenten und Inhalte wie urheberrechtlich geschützte Inhalte und/oder Websites von Drittanbietern (nachfolgend „Drittprodukte und -dienste“ genannt). BlackBerry hat keinen Einfluss auf und übernimmt keine Haftung für Drittprodukte und -dienste, dies gilt u. a. für Inhalt, Genauigkeit, Einhaltung der Urheberrechtsgesetze, Kompatibilität, Leistung, Zuverlässigkeit, Rechtmäßigkeit, Angemessenheit, Links oder andere Aspekte der Drittprodukte und -dienste. Der Einschluss eines Verweises auf Drittprodukte und -dienste in dieser Dokumentation impliziert in keiner Weise eine besondere Empfehlung der Drittprodukte und -dienste oder des Drittanbieters durch BlackBerry.

SOFERN ES NICHT DURCH DAS IN IHREM RECHTSGEBIET GELTENDE RECHT AUSDRÜCKLICH UNTERSAGT IST, WERDEN HIERMIT SÄMTLICHE AUSDRÜCKLICHEN ODER KONKLUDENTEN BEDINGUNGEN, BILLIGUNGEN, GARANTIEN, ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN JEDER ART, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF BEDINGUNGEN, BILLIGUNGEN, GARANTIEN, ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN HINSICHTLICH DER HALTBARKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER VERWENDUNGSZWECK, MARKTGÄNGIGKEIT, MARKTGÄNGIGEN QUALITÄT, NICHTVERLETZUNG VON RECHTEN DRITTER, ZUFRIEDENSTELLENDEN QUALITÄT ODER DES EIGENTUMSRECHTS ABGELEHNT. DIES GILT AUCH FÜR ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN, DIE SICH AUS EINEM GESETZ, EINER GEPFLOGENHEIT, CHANCEN BZW. HANDELSGEPFLOGENHEITEN ERGEBEN ODER IM ZUSAMMENHANG MIT DER DOKUMENTATION ODER IHRER VERWENDUNG, DER LEISTUNG ODER MANGELNDEN LEISTUNG VON SOFTWARE, HARDWARE, DIENSTEN ODER DRITTPRODUKTEN UND -DIENSTEN STEHEN, AUF DIE HIER VERWIESEN WIRD. MÖGLICHERWEISE GELTEN FÜR SIE ZUDEM ANDERE LANDESSPEZIFISCHE RECHTE. IN MANCHEN RECHTSGEBIETEN IST DER AUSSCHLUSS ODER DIE EINSCHRÄNKUNG KONKLUDENTER GEWÄHRLEISTUNGEN UND BEDINGUNGEN NICHT ZULÄSSIG. IN DEM GESETZLICH ZULÄSSIGEN UMFANG WERDEN SÄMTLICHE KONKLUDENTEN GEWÄHRLEISTUNGEN ODER BEDINGUNGEN IM ZUSAMMENHANG MIT DER DOKUMENTATION, DIE EINGESCHRÄNKT WERDEN KÖNNEN, SOFERN SIE NICHT WIE OBEN DARGELEGT AUSGESCHLOSSEN WERDEN KÖNNEN, HIERMIT AUF 90 TAGE AB DATUM DES ERWERBS DER DOKUMENTATION ODER DES ARTIKELS, AUF DEN SICH DIE FORDERUNG BEZIEHT, BESCHRÄNKT.

IN DEM DURCH DAS IN IHREM RECHTSGEBIET ANWENDBARE GESETZ MAXIMAL ZULÄSSIGEN AUSMASS HAFTET BLACKBERRY UNTER KEINEN UMSTÄNDEN FÜR SCHÄDEN JEGLICHER ART, DIE IM ZUSAMMENHANG MIT DIESER DOKUMENTATION ODER IHRER VERWENDUNG, DER LEISTUNG ODER NICHTLEISTUNG JEGLICHER SOFTWARE, HARDWARE, DIENSTE ODER DRITTPRODUKTE UND -DIENSTE, AUF DIE HIER BEZUG GENOMMEN WIRD, STEHEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE FOLGENDEN SCHÄDEN: DIREKTE,

VERSCHÄRFTEN SCHADENERSATZ NACH SICH ZIEHENDE, BEILÄUFIG ENTSTANDENE, INDIREKTE, KONKRETE, STRAFE EINSCHLIESSENDE SCHÄDEN, FOLGESCHÄDEN ODER SCHÄDEN, FÜR DIE ANSPRUCH AUF KOMPENSATORISCHEN SCHADENERSATZ BESTEHT, SCHÄDEN WEGEN ENTGANGENEN GEWINNEN ODER EINKOMMEN, NICHTREALISIERUNG ERWARTETER EINSPARUNGEN, BETRIEBSUNTERBRECHUNGEN, VERLUST GESCHÄFTLICHER DATEN, ENTGANGENE GESCHÄFTSCHANCEN ODER BESCHÄDIGUNG BZW. VERLUST VON DATEN, DAS UNVERMÖGEN, DATEN ZU ÜBERTRAGEN ODER ZU EMPFANGEN, PROBLEME IM ZUSAMMENHANG MIT ANWENDUNGEN, DIE IN VERBINDUNG MIT BLACKBERRY-PRODUKTEN UND -DIENSTEN VERWENDET WERDEN, KOSTEN VON AUSFALLZEITEN, NICHTVERWENDBARKEIT VON BLACKBERRY-PRODUKTEN UND -DIENSTEN ODER TEILEN DAVON BZW. VON MOBILFUNKDIENSTEN, KOSTEN VON ERSATZGÜTERN, DECKUNG, EINRICHTUNGEN ODER DIENSTEN, KAPITAL- ODER ANDERE VERMÖGENSSCHÄDEN, UNABHÄNGIG DAVON, OB SCHÄDEN DIESER ART ABZUSEHEN ODER NICHT ABZUSEHEN WAREN, UND AUCH DANN, WENN BLACKBERRY AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE.

IN DEM DURCH DAS IN IHREM RECHTSGEBIET ANWENDBARE GESETZ MAXIMAL ZULÄSSIGEN AUSMASS ÜBERNIMMT BLACKBERRY KEINERLEI VERANTWORTUNG, VERPFLICHTUNG ODER HAFTUNG, SEI SIE VERTRAGLICHER, DELIKTRECHTLICHER ODER ANDERWEITIGER NATUR, EINSCHLIESSLICH DER HAFTUNG FÜR FAHRLÄSSIGKEIT UND DER DELIKTSHAFTUNG.

DIE IN DIESEM DOKUMENT GENANNTEN EINSCHRÄNKUNGEN, AUSSCHLÜSSE UND HAFTUNGSAUSSCHLÜSSE GELTEN (A) UNGEACHTET DER VON IHNEN ANGEFÜHRTEN KLAGEGRÜNDE, FORDERUNGEN ODER KLAGEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF VERTRAGSBRUCH, FAHRLÄSSIGKEIT, ZIVILRECHTLICHER DELIKTE, DELIKTSHAFTUNG ODER SONSTIGE RECHTSTHEORIE UND SIND AUCH NACH EINEM WESENTLICHEN VERSTOSS BZW. EINEM FEHLENDEN GRUNDLEGENDEN ZWECK DIESER VEREINBARUNG ODER EINES DARIN ENTHALTENEN RECHTSBEHELFS WIRKSAM; UND GELTEN (B) FÜR BLACKBERRY UND DIE ZUGEHÖRIGEN UNTERNEHMEN, RECHTSNACHFOLGER, BEVOLLMÄCHTIGTEN, VERTRETER, LIEFERANTEN (EINSCHLIESSLICH MOBILFUNKANBIETERN), AUTORISIERTE BLACKBERRY-DISTRIBUTOREN (EBENFALLS EINSCHLIESSLICH MOBILFUNKANBIETERN) UND DIE JEWEILIGEN FÜHRUNGSKRÄFTE, ANGESTELLTEN UND UNABHÄNGIGEN AUFTRAGNEHMER.

ZUSÄTZLICH ZU DEN OBEN GENANNTEN EINSCHRÄNKUNGEN UND AUSSCHLÜSSEN HAFTEN DIE FÜHRUNGSKRÄFTE, ANGESTELLTEN, VERTRETER, DISTRIBUTOREN, LIEFERANTEN, UNABHÄNGIGEN AUFTRAGNEHMER VON BLACKBERRY ODER BLACKBERRY ANGEHÖRENDEN UNTERNEHMEN IN KEINER WEISE IM ZUSAMMENHANG MIT DER DOKUMENTATION.

Bevor Sie Drittprodukte bzw. -dienste abonnieren, installieren oder verwenden, müssen Sie sicherstellen, dass Ihr Mobilfunkanbieter sich mit der Unterstützung aller zugehörigen Funktionen einverstanden erklärt hat. Einige Mobilfunkanbieter bieten möglicherweise keine Internet-Browsing-Funktion in Zusammenhang mit einem Abonnement für den BlackBerry® Internet Service an. Erkundigen Sie sich bei Ihrem Dienstanbieter bezüglich Verfügbarkeit, Roaming-Vereinbarungen, Mobilfunktarifen und Funktionen. Für die Installation oder Verwendung von Drittprodukten und -diensten mit den Produkten und Diensten von BlackBerry sind u. U. Patent-, Marken-, Urheberrechts- oder sonstige Lizenzen erforderlich, damit die Rechte Dritter nicht verletzt werden. Es liegt in Ihrer Verantwortung, zu entscheiden, ob Sie Drittprodukte und -dienste verwenden möchten, und festzustellen, ob hierfür Lizenzen erforderlich sind. Für den Erwerb etwaiger Lizenzen sind Sie verantwortlich. Installieren oder verwenden Sie Drittprodukte und -dienste erst nach dem Erwerb aller erforderlichen Lizenzen. Alle Drittprodukte und -dienste, die Sie mit Produkten und Diensten von BlackBerry erhalten, werden lediglich zu Ihrem Vorteil, OHNE MÄNGELGEWÄHR und ohne ausdrückliche oder stillschweigende Bedingung, Billigung, Garantie, Zusicherung oder Gewährleistung jedweder Art von BlackBerry bereitgestellt. BlackBerry übernimmt in diesem Zusammenhang keinerlei Haftung. Die Verwendung von Drittprodukten und -diensten unterliegt Ihrer Zustimmung zu den Bedingungen separater Lizenzen und anderer geltender Vereinbarungen mit Dritten, sofern sie nicht ausdrücklich von einer Lizenz oder anderen Vereinbarung mit BlackBerry abgedeckt wird.

Die Nutzungsbedingungen für BlackBerry-Produkte und -Dienste werden in einer entsprechenden separaten Lizenz oder anderen Vereinbarung mit BlackBerry dargelegt. KEINE PASSAGE IN DIESEM DOKUMENT IST DAZU VORGESEHEN, BELIEBIGE SCHRIFTLICHE VEREINBARUNGEN ODER GARANTIEN, DIE VON BLACKBERRY FÜR TEILE VON BELIEBIGEN BLACKBERRY-PRODUKTEN ODER -DIENSTLEISTUNGEN AN ANDERER STELLE ALS IN DIESER DOKUMENTATION ANGEGEBEN WURDEN, ZU ERSETZEN.

BlackBerry Enterprise Software enthält bestimmte Softwarekomponenten von Drittanbietern. Die mit der Software verbundenen Lizenz- und Copyright-Informationen finden Sie unter: http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

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

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

Veröffentlicht in Kanada