Cylance Endpoint Security

CylancePROTECT Desktop 3.x Upgrade Handbuch

Contents

Vorteile des Upgrades auf CylancePROTECT Desktop 3.x

CylancePROTECT Desktop Version 3.x stellt für das Produkt einen bedeutenden Fortschritt dar und bietet neue Funktionen und Verbesserungen der Benutzerfreundlichkeit ein, um die Sicherheit der Daten und Geräte Ihres Unternehmens zu gewährleisten.

Wenn Sie auf CylancePROTECT Desktop für 3.x aktualisieren, erhalten Sie Zugriff auf die folgenden Funktionen:

Windows

Funktion	Beschreibung
Betriebssystemkompatibilität	Der Windows 3.x-Agent bietet Unterstützung für Windows 11. Weitere Informationen finden Sie in der CylancePROTECT Desktop-Kompatibilitätsmatrix.
Agenten-Verbesserungen	• Der Windows3.1-Agent wird als vertrauenswürdiger Dienst unter Verwendung der AM-PPL-Technologie (Antimalware Protected Process Light) von Microsoft ausgeführt, die die Sicherheitsprozesse des Agenten vor bösartigen Aktionen schützt. So kann beispielsweise der Agent vor dem Abbruch geschützt werden. Für diese Funktion muss auf dem Endgerät Windows 10 1709 oder höher oder Windows Server 2019 oder höher ausgeführt werden. • Der Windows 3.2-Agent meldet eine Liste der auf Endgeräten installierten Anwendungen an die Verwaltungskonsole. Mit dieser Funktion können Administratoren auf Endgeräten installierte Anwendungen identifizieren, die eine Quelle für Schwachstellen sein könnten, und Maßnahmen zur Behebung von Schwachstellen nach Priorität ordnen und diese entsprechend angehen. Administratoren können alle Anwendungen anzeigen, die auf Endgeräten installiert sind, die bei dem Mandanten registriert sind, und eine Liste der Anwendungen anzeigen, die auf einzelnen Endgeräten installiert sind. Diese Funktion kann in der Geräterichtlinie (Agenten-Einstellungen) aktiviert werden.

Funktion	Beschreibung
Verbesserungen des Speicherschutzes	• Es wurden neue Funktionen zu Verletzungstypen hinzugefügt, wodurch weitere Ereignisse generiert werden. • Der Verletzungstyp „Injektion über APC“ ist in den Speicherschutzeinstellungen einer Geräterichtlinie verfügbar. Mit dieser Option kann CylancePROTECT Desktop einen Prozess erkennen, der über einen asynchronen Prozeduraufruf (Asynchronous Procedure Call, APC) beliebigen Code in den Zielprozess injiziert. Weitere Informationen finden Sie in KB 92422. • Der Verletzungstyp „Änderung der Speicherberechtigung bei untergeordneten Prozessen“ ist in den Speicherschutzeinstellungen einer Geräterichtlinie verfügbar. Mit dieser Option kann CylancePROTECT Desktop erkennen, wann ein Verletzungsprozess einen untergeordneten Prozess erstellt und die Speicherzugriffsberechtigungen in diesem untergeordneten Prozess geändert hat. • Die Benutzerfreundlichkeit der Speicherschutzsteuerungen wurde verbessert. • Verbesserte Erkennung von LSASS-Leseverletzungen für Windows-Geräte. • Die Größenbeschränkung für Ausschlüsse zum Speicherschutz wurde von 64 KB auf 2 MB erhöht, sodass Sie weitere Ausschlüsse hinzufügen können. • Ausnahmen für Anwendungs-DLLs von Drittanbietern werden jetzt unterstützt, damit Anwendungen von Drittanbietern neben CylancePROTECT Desktop ausgeführt werden können. Wenn Sie beispielsweise Sicherheitsprodukte von Drittanbietern zusätzlich zu CylancePROTECT ausführen, können Sie einen Ausschluss für die entsprechenden .dll-Dateien hinzufügen, damit CylancePROTECT bestimmte Verstöße für diese Produkte ignoriert. Für diese Funktion ist Agent-Version 3.1.1001 oder höher erforderlich. Weitere Informationen finden Sie unter der Einstellung „Als DLL-Ausschluss behandeln“ in der Richtlinie für Speicherschutzgeräte. • Der Speicherschutzsensor für den Verletzungstyp „Schädliche Payload“ wurde verbessert, um die Genauigkeit der Meldung von Verstößen zu verbessern und unnötige Warnungen zu reduzieren. Für diese Funktion ist Agent-Version 3.1.1001 oder höher erforderlich.
Verbesserungen beim Schutz	• Der Windows 3.1-Agent ermöglicht es Administratoren, ein benutzerdefiniertes Intervall für die Ausführung von Bedrohungsscans im Hintergrund über die Geräterichtlinie (Schutzeinstellungen) festzulegen. Das Scanintervall kann zwischen 1 und 90 Tagen betragen. Das Standard-Scanintervall beträgt 10 Tage. Beachten Sie, dass eine Erhöhung der Häufigkeit der Scans die Leistung des Geräts beeinträchtigen kann. • Der Windows 3.2-Agent unterstützt Administratoren bei Bedarf bei der Initiierung eines Scans zur Bedrohungserkennung im Hintergrund von der Verwaltungskonsole aus. Der Befehl kann über den Bildschirm mit den Gerätedetails für ein einzelnes Gerät oder für mehrere Geräte gleichzeitig über den Geräte-Bildschirm gesendet werden. • Das Datum des letzten Scans für jedes Gerät wird in der Verwaltungskonsole protokolliert.

Funktion	Beschreibung
Verbesserungen der Skriptsteuerung	• Sie können auswählen, ob CylancePROTECT Desktop bei Python-Skripten (2.7, 3.0 bis 3.8) und .NET DLR (z. B. IronPython) eine Warnung ausgeben oder diese blockieren soll. Sie können die Skriptsteuerung für diese Skripttypen auch deaktivieren. • Eingebettete VB-Skripte, die Skriptsteuerungsereignisse verursacht haben, wurden in der Agentenversion 2.1.1580 blockiert; die Erkennung von Verletzungen der eingebetteten VB-Skriptsteuerung wurde in Agent 3.0.1000 und höher deaktiviert. • Der Windows 3.1-Agent arbeitet mit der Anti-Malware-Scan-Schnittstelle (AMSI) von Microsoft, sodass bei der Ausführung eines potenziell gefährlichen XLM-Makros Bedrohungsinformationen an die Verwaltungskonsole gemeldet werden und der Agent gemäß den Regeln der Geräterichtlinie für Skriptsteuerungsereignisse auf die Schnittstelle antwortet. Der Agent antwortet beispielsweise, ob er die Ausführung des Makros zulässt oder blockiert. Diese Funktion wird über die Einstellung „Skriptsteuerung > XLM-Makros“ in der Geräterichtlinie aktiviert und erfordert, dass auf dem Gerät Windows 10 ausgeführt wird. Stellen Sie sicher, dass VBA-Makros im Menü Excel **Datei > Vertrauensstellungscenter > Excel-Vertrauensstellungscenter > „Makroeinstellungen“** deaktiviert sind. • Der Windows-Agent meldet übergeordnete und Interpreter-Prozesse an die Cylance-Konsole, wenn ein potenziell bösartiges Skript ausgeführt wird. Administratoren können Ausschlüsse für einen übergeordneten Prozess oder einen Interpreter-Prozess eines Skripts hinzufügen, damit das Skript auf einem Gerät ausgeführt werden kann. Für diese Funktion ist Agent-Version 3.1.1001 erforderlich. • Der Windows 3.2-Agent unterstützt eine erweiterte Skriptsteuerung mit Skriptauswertung. Die Ausführung von Skripten mit einer unsicheren oder abnormalen Bedrohungsauswertung kann intelligent gesperrt werden und es kann eine entsprechende Warnung an die Verwaltungskonsole gesendet werden. Administratoren können die Einstellungen für die Skriptsteuerung in der Geräterichtlinie so konfigurieren, dass Skripte blockiert werden, die CylancePROTECT als unsicher oder abnormal erkennt. • Der Windows 3.2-Agent unterstützt den Warnungsmodus für PowerShell-Konsolenskripte, sodass erkannte Ereignisse an die Verwaltungskonsole gemeldet werden, während sie weiterhin ausgeführt werden können. Administratoren können die Einstellung über die Registerkarte „Skriptsteuerung“ in der Geräterichtlinie über das Drop-Down-Menü für die PowerShell-Konsole steuern.

Funktion	Beschreibung
Verbesserungen bei der Makroerkennung	• In Geräterichtlinien wurde die Makroerkennungsfunktion für Windows-Geräte von der Registerkarte „Skriptsteuerung“ auf die Registerkarte „Speicheraktionen“ (Exploitation > Gefährliche VBA-Makros) für Geräte mit Windows-Agentenversion 2.1.158x oder höher verschoben. Die vorherige Skriptsteuerungsoption für Version 2.1.1578 und niedriger unterstützt die Aktionen „Warnung“ und „Blockieren“; die neue Speicherschutzoption unterstützt die Aktionen „Ignorieren“, „Warnung“, „Blockieren“ und „Beenden“. • Sie können jetzt in den Speicherschutzeinstellungen einer Geräterichtlinie Ausschlüsse für den Typ „Gefährliche VBA-Makros“ hinzufügen. • Dateien, die Verletzungen im Zusammenhang mit gefährlichen VBA-Makros verursachen, werden in der Verwaltungskonsole angezeigt, sodass Sie die entsprechenden Dokumente identifizieren und bestimmen können, ob Sie sie der Ausschlussliste hinzufügen müssen.
Verbesserungen der Gerätesteuerung	Sie können jetzt schreibgeschützten Zugriff auf die folgenden USB-Gerätetypen zulassen: • Digitalbild • USB CD/DVD RW • USB-Laufwerk • VMware USB-Passthrough • Tragbares Windows-Gerät
Verbesserungen der globalen sicheren Liste	Durch das Hinzufügen eines SHA256-Hashes zur globalen sicheren Liste für Skripte wird nun verhindert, dass Blockierungsereignisse, die mit diesem Hash in Verbindung stehen, in der Verwaltungskonsole angezeigt werden.
Protokollierung von Änderungen	Wichtige Protokolleinträge wurden von der Debug-Protokollebene in die Info-Protokollebene verschoben.

Linux

Funktion	Beschreibung
Betriebssystemkompatibilität	Der Linux 3.2.x-Agent unterstützt die folgenden Linux-Distributionen: • Amazon Linux 2023 • Amazon Linux 2, Kernel 5.10 Der Linux 3.1.x-Agent unterstützt die folgenden Linux-Distributionen: • Red Hat Enterprise Linux 9 und 9.1 • Oracle 9 und 9.1 • Oracle UEK 9 und 9.1 • Oracle 8.7 • Oracle UEK 8.7 • SUSE Linux Enterprise Server (SLES) 15 SP4 • Ubuntu 22.04 LTS Der Linux 3.0.x-Agent unterstützt die folgenden Linux-Distributionen: • Red Hat Enterprise Linux /CentOS 8.4 • Red Hat Enterprise Linux 8.5 • Oracle 8.4 • SUSE (SLES) 12 SP5 • SUSE (SLES) 15 SP2 und SP3 Weitere Informationen finden Sie in der Kompatibilitätsmatrix für CylancePROTECT Desktop. Um die vollständige Liste der unterstützten Linux-Kernels und -Treiber anzuzeigen, laden Sie die Tabelle der unterstützten Linux-Kernels herunter.
Scan auf Abruf zur Bedrohungserkennung im Hintergrund	Administratoren können nun von der Verwaltungskonsole aus einen Scan auf Abruf zur Bedrohungserkennung im Hintergrund starten. Der Befehl kann über den Bildschirm mit den Gerätedetails für ein einzelnes Gerät oder für mehrere Geräte gleichzeitig über den Geräte-Bildschirm gesendet werden. Für diese Funktion ist ein CylancePROTECT Desktop-Agent der Version 3.2 erforderlich. Das Datum des letzten Scans für jedes Gerät wird in der Verwaltungskonsole protokolliert.
Benutzerdefiniertes Intervall für die Überprüfung der Bedrohungserkennung im Hintergrund	• Administratoren können ein benutzerdefiniertes Intervall für die Ausführung von Scans zur Erkennung von Bedrohungen im Hintergrund über die Geräterichtlinie festlegen. Das Scanintervall kann zwischen 1 und 90 Tagen betragen. Das Standard-Scanintervall beträgt 10 Tage. • Für diese Funktion ist ein CylancePROTECT Desktop-Agent der Version 3.1 erforderlich. • Das Datum des letzten Scans für jedes Gerät wird in der Verwaltungskonsole protokolliert.

Funktion	Beschreibung
Linux-Treiber automatisch aktualisieren	• Der CylancePROTECT Desktop-Agent 3.1.1000 für Linux-Geräte kann jetzt eine Aktualisierung auf den neuesten unterstützten Agent-Treiber anfordern, wenn ein aktualisierter Kernel auf dem System erkannt wird. Wenn beispielsweise der Linux-Kernel aktualisiert wird und der aktuell installierte Agent-Treiber dies nicht unterstützt, kann der Agent den Treiber jetzt automatisch aktualisieren, sobald ein kompatibler Treiber veröffentlicht wird. • Für diese Funktion ist der CylancePROTECT Desktop-Agent Version 3.1.1000 und die Agent-Treiberversion 3.1.1000 oder höher erforderlich. • Um diese Funktion zu aktivieren, wählen Sie die Option Linux-Treiber automatisch aktualisieren in der zonenbasierten Aktualisierungsregel im Menü Einstellungen > Aktualisieren in der Verwaltungskonsole aus.
Verbesserungen des Speicherschutzes	• Es wurden neue Funktionen zu Verletzungstypen hinzugefügt, wodurch weitere Ereignisse generiert werden. • Die Benutzerfreundlichkeit der Speicherschutzsteuerungen wurde verbessert. • Die Größenbeschränkung für Ausschlüsse zum Speicherschutz wurde von 64 KB auf 2 MB erhöht, sodass Sie weitere Ausschlüsse hinzufügen können.

macOS

Funktion	Beschreibung
Betriebssystemkompatibilität	• Der CylancePROTECT Desktop 3.2.x-Agent bietet Unterstützung für macOS 14 (Sonoma). • Der CylancePROTECT Desktop 3.1.x-Agent bietet Unterstützung für macOS 13 (Ventura). • Der CylancePROTECT Desktop 3.0.x-Agent bietet Unterstützung für macOS 12 (Monterey).
Scan auf Abruf zur Bedrohungserkennung im Hintergrund	Administratoren können nun von der Verwaltungskonsole aus einen Scan auf Abruf zur Bedrohungserkennung im Hintergrund starten. Der Befehl kann über den Bildschirm mit den Gerätedetails für ein einzelnes Gerät oder für mehrere Geräte gleichzeitig über den Geräte-Bildschirm gesendet werden. Für diese Funktion ist ein CylancePROTECT Desktop-Agent der Version 3.2 erforderlich. Das Datum des letzten Scans für jedes Gerät wird in der Verwaltungskonsole protokolliert.
Benutzerdefiniertes Intervall für die Überprüfung der Bedrohungserkennung im Hintergrund	• Administratoren können ein benutzerdefiniertes Intervall für die Ausführung von Scans zur Erkennung von Bedrohungen im Hintergrund über die Geräterichtlinie festlegen. Das Scanintervall kann zwischen 1 und 90 Tagen betragen. Das Standard-Scanintervall beträgt 10 Tage. • Das Datum des letzten Scans für jedes Gerät wird in der Verwaltungskonsole protokolliert.

Funktion	Beschreibung
Verbesserungen des Speicherschutzes	• Es wurden neue Funktionen zu Verletzungstypen hinzugefügt, wodurch weitere Ereignisse generiert werden. • Die Benutzerfreundlichkeit der Speicherschutzsteuerungen wurde verbessert. • Die Größenbeschränkung für Ausschlüsse zum Speicherschutz wurde von 64 KB auf 2 MB erhöht, sodass Sie weitere Ausschlüsse hinzufügen können.

Weitere Informationen zu zusätzlichen Funktionen für die neuesten 3.x-Agenten sowie eine umfassende Liste behobener Probleme finden Sie in den Versionshinweisen zu Cylance Endpoint Security.

Um von diesen Erweiterungen und den Verbesserungen in zukünftigen Versionen von CylancePROTECT Desktop zu profitieren, empfiehlt BlackBerry dringend, alle Geräte mit dem Agenten 2.x.158x oder niedriger auf die neueste Version des Agenten 3.x zu aktualisieren. Dieser Leitfaden enthält Überlegungen und zusätzliche Anweisungen für ein erfolgreiches Upgrade.

Upgrade auf CylancePROTECT Desktop 3.x

Dieser Abschnitt enthält eine Schritt-für-Schritt-Anleitung und Best Practices für ein erfolgreiches Upgrade auf CylancePROTECT Desktop Version 3.x.

Schritt	Aktion
1	Lesen Sie die Anleitung unter Vorbereiten Ihrer Testumgebung.
2	Prüfen Sie die Upgrade-Pfade für Agenten, um den spezifischen Pfad zu bestimmen, den Sie befolgen müssen.
3	Konfigurieren und Testen des Speicherschutzes.
4	Konfigurieren und Testen der Makroerkennung (nur Windows).
5	Migrieren Sie bei Bedarf Makroausschlüsse für die Skriptsteuerung in die neue Speicherschutz-Konfiguration.
6	Nachdem Sie die Tests und die Validierung in der Testumgebung abgeschlossen haben, wenden Sie die aktualisierten Geräterichtlinien auf Ihre Produktionsumgebung an.

Vorbereiten Ihrer Testumgebung

- BlackBerry empfiehlt, das Upgrade auf CylancePROTECT Desktop für Windows 3.x in einer speziellen Testzone zu testen, bevor Sie das Upgrade in Ihrer Produktionsumgebung bereitstellen. Weitere Informationen zu Zonen finden Sie unter Einrichten von Zonen in der Dokumentation zur Einrichtung von Cylance Endpoint Security.
- Richten Sie Ihre Testgeräte mit den Apps und Konfigurationen ein, die Ihre Produktionsumgebung genau widerspiegeln.
- Erstellen Sie spezielle Geräterichtlinien, die Sie für Ihre Testzonen und Geräte verwenden. Sie können neue Geräterichtlinien erstellen oder vorhandene Richtlinien kopieren und ändern.
- Konfigurieren Sie zonenbasierte Aktualisierungsregeln in der Verwaltungskonsole, um das 3.x-Upgrade auf die speziellen Zonen und Geräte zu beschränken, die Sie für Tests verwenden möchten. Anweisungen hierzu finden Sie unter Verwalten von Updates für die CylancePROTECT Desktop- und CylanceOPTICS-Agenten in der Dokumentation zur Einrichtung von Cylance Endpoint Security.
- BlackBerry empfiehlt, das Support Collection Tool aus KB 66596 herunterzuladen. Wenn Sie sich an den BlackBerry-Support wenden, werden Sie möglicherweise aufgefordert, das Tool auszuführen, um zusätzliche Daten zu erfassen.
- Unter Upgrade-Pfade für Agenten finden Sie den spezifischen Pfad, den Sie befolgen müssen.
- Nachdem Sie die Konfigurations- und Testaktivitäten in diesem Handbuch abgeschlossen und das Upgrade in Ihren Testzonen validiert haben, können Sie das Agenten-Upgrade und die aktualisierten Geräterichtlinien auf Ihre Produktionsumgebung anwenden.

Upgrade-Pfade für den CylancePROTECT Desktop-3.x-Agenten

Die folgenden Upgrade-Pfade wurden getestet und werden offiziell unterstützt:

Upgrade-Pfad auf Windows-Agent Version 3.x

Aktuelle Agentenversion	Upgrade-Pfad
2.0.154x	→ 2.1.157x → 3.1 → 3.2.1000
2.1.156x	→ 2.1.157x → 3.1 → 3.2.1000
2.1.157x	→ 3.1 → 3.2.1000
2.1.158x	→ 3.2.1000
3.0	→ 3.2.1000
3.1	→ 3.2.1000

Upgrade-Pfad auf Linux-Agent Version 3.x

Aktuelle Agentenversion	Upgrade-Pfad
2.1.157x oder früher	→ 2.1.158x → 2.1.159x → 3.2.1000
2.1.158x	→ 2.1.159x → 3.2.1000
2.1.159x	→ 3.2.1000
3.0	→ 3.2.1000
3.1	→ 3.2.1000

Upgrade-Pfad auf macOS-Agent Version 3.x

Aktuelle Agentenversion	Upgrade-Pfad
2.0.154x	→ 2.1.156x → 2.1.158x → 3.2.1000
2.1.156x	→ 2.1.158x → 3.2.1000
2.1.158x	→ 3.2.1000
2.1.159x	→ 3.2.1000
3.0	→ 3.2.1000

Aktuelle Agentenversion	Upgrade-Pfad
3.1	→ 3.2.1000

Konfigurieren und Testen des Speicherschutzes

CylancePROTECT Desktop 3.x bietet verschiedene Verbesserungen beim Speicherschutz und einen besseren Einblick in die Aktivitäten der Anwendungen und Prozesse auf einem Gerät. In manchen Situationen führen Anwendungen Vorgänge aus, die als schädlich angesehen werden könnten, aber für legitime Zwecke ausgeführt werden. BlackBerry empfiehlt die folgenden Schritte und Best Practices, um den CylancePROTECT Desktop 3.x-Agenten richtig einzustellen, bevor Sie ihn in Ihrer Produktionsumgebung bereitstellen. Weitere Informationen zu Speicherschutz-Verletzungstypen finden Sie unter Speicherschutz in der Dokumentation zur Einrichtung von Cylance Endpoint Security.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien > Geräterichtlinie**.
2. Klicken Sie auf die Geräterichtlinie für Ihre Testgeräte.
3. Aktivieren Sie auf der Registerkarte **Speicheraktionen** das Kontrollkästchen **Speicherschutz**.
4. Erweitern Sie in der Tabelle **Verletzungstyp** die Einträge **Exploitation**, **Prozessinjektion** und **Eskalation**. Wählen Sie für alle Verletzungstypen, die unter **Verfügbar für Agentenversion 2.1.1580 und höher** und **Verfügbar für CylancePROTECT 3.0 und höher** aufgeführt sind, die Aktion **WARNUNG** aus.
5. Speichern Sie die Geräterichtlinie.
6. Führen Sie CylancePROTECT Desktop 3.x auf Ihren Testgeräten aus und überprüfen Sie die Warnungen, um das Risiko dieser Exploits in Ihrer Umgebung zu bestimmen. Wenn eine dieser Warnungen ein geringes Risiko aufweist und Auswirkungen auf das Geschäft hat, können Sie gezielte Ausschlüsse für den Speicherschutz hinzufügen. Anweisungen und Anleitungen finden Sie unter Speicherschutz.

   Es wird empfohlen, jedes Testgerät nach der Installation oder dem Upgrade auf CylancePROTECT Desktop 3.x neu zu starten.

Wenn Sie fertig sind: Nachdem Sie die Warnungen überprüft und die erforderlichen Ausschlüsse hinzugefügt haben, können Sie die Aktionen der Verletzungstypen in der Geräterichtlinie nach Bedarf ändern (z. B. „Blockieren“ oder „Beenden“).

Konfigurieren und Testen der Makroerkennung (nur Windows)

In einer Geräterichtlinie stehen zwei Optionen zur Verfügung, um potenziell gefährliche Makros auf Windows-Geräten zu erkennen und darauf zu reagieren. Die Makro-Option auf der Registerkarte „Skriptsteuerung“ gilt für Windows-Agenten 2.1.1578 und niedriger. Die neue Option „Exploitation > Gefährliches VBA-Makro“ auf der Registerkarte „Speicheraktionen“ gilt für Windows-Agenten 2.1.1580 und höher. Wenn Sie Ihr Upgrade auf Agent 3.x testen, müssen Sie Ihre aktuelle Konfiguration für die Erkennung von und Reaktion auf Makros überprüfen und die neue Option „Gefährliche VBA-Makros“ entsprechend konfigurieren.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien > Geräterichtlinie**.
2. Klicken Sie auf die Richtlinie für Ihr Produktionsgerät.
3. Beachten Sie auf der Registerkarte **Skriptsteuerung** die aktuelle Konfiguration für Makros (Warnung oder Blockieren).
4. Klicken Sie unter **Richtlinien > Geräterichtlinie** auf die Geräterichtlinie für Ihre Testgeräte.
5. Erweitern Sie auf der Registerkarte **Speicheraktionen** die Option **Exploitation**.

6. Legen Sie für die Verletzung **Gefährliche VBA-Makros** die entsprechende Aktion fest (Ignorieren, Warnung, Blockieren oder Beenden).
7. Speichern Sie die Geräterichtlinie.
8. Migrieren Sie bei Bedarf Makroausschlüsse für die Skriptsteuerung in die neue Speicherschutz-Konfiguration.
9. Führen Sie CylancePROTECT Desktop 3.x auf Testgeräten aus, die Dateien mit Makros verwenden, die in Ihrem Unternehmen häufig verwendet werden. Fügen Sie bei Bedarf zusätzliche Speicherschutz-Ausschlüsse für sichere Makros hinzu. Anweisungen und Anleitungen finden Sie unter Speicherschutz in der Dokumentation zur Einrichtung von Cylance Endpoint Security.

Migrieren von Makroausschlüssen für die Skriptsteuerung in die neue Speicherschutz-Konfiguration (nur Windows)

Wenn Sie zuvor Makroausschlüsse auf der Registerkarte „Skriptsteuerung“ Ihrer Geräterichtlinien hinzugefügt haben, müssen Sie diese Ausschlüsse in die neue Speicherschutz-Konfiguration für CylancePROTECT Desktop Windows 3.x migrieren. Wenn Sie die Ausschlüsse für die Skriptsteuerung manuell migrieren möchten, können Sie einfach die Ausschlüsse aufzeichnen, die Sie auf der Registerkarte „Skriptsteuerung“ Ihrer Geräterichtlinien hinzugefügt haben, und dann dieselben Ausschlüsse auf der Registerkarte „Speicheraktionen“ in Ihren Geräterichtlinien hinzufügen.

Führen Sie die folgenden Schritte aus, wenn Sie die vorhandenen Ausschlüsse für die Skriptsteuerung mit einem PowerShell-Skript migrieren möchten, das von BlackBerry bereitgestellt wird.

Hinweis: Die folgenden Schritte gelten für Mandanten, die mit der Cylance-Konsole verwaltet werden. Wenn Sie Mandanten über die mehrmandantenfähige Konsole verwalten, siehe KB 92149.

Bevor Sie beginnen:

- Stellen Sie sicher, dass PowerShell auf Ihrem Computer installiert ist und dass die PowerShell-Skripte nicht durch Sicherheitssoftware blockiert sind, einschließlich CylancePROTECT Desktop. Wenn CylancePROTECT Desktop auf Ihrem Computer installiert ist, stellen Sie in der Geräterichtlinie sicher, die Ihrem Gerät zugewiesen ist, dass **Skriptsteuerung > Verwendung der PowerShell-Konsole blockieren** deaktiviert ist.
- Fügen Sie in der Cylance-Konsole eine Integration mit den folgenden API-Berechtigungen hinzu und erfassen Sie die resultierende Anwendungs-ID und den geheimen Anwendungsschlüssel:
  - **Richtlinien**: Lesen, Ändern
  - **Benutzer**: Lesen
- Erfassen Sie unter **Einstellungen > Integrationen** die **Mandanten-ID**.
- Wenn Sie das Skript ausführen, geben Sie die E-Mail-Adresse eines Administratorkontos für die Cylance-Konsole an. Stellen Sie sicher, dass das Konto, das Sie verwenden möchten, über Administratorrechte verfügt.
- Überprüfen Sie in den Geräterichtlinien, in denen Sie Ausschlüsse von der Skriptsteuerung zum Speicherschutz migrieren möchten, ob die Skriptsteuerung aktiviert ist und ob Makroausschlüsse vorhanden sind.
  - Das Skript ignoriert Richtlinien, bei denen die Skriptsteuerung deaktiviert ist, und Richtlinien, für die keine Ausschlüsse definiert wurden.
  - Das Skript migriert keine Ausschlüsse mit Multibyte-Zeichen. Sie müssen diese Ausschlüsse manuell hinzufügen.
- Laden Sie das PowerShell-Skript herunter.

1. Öffnen Sie eine PowerShell-Eingabeaufforderung und ändern Sie das Verzeichnis zum Speicherort des Skripts.
2. Führen Sie das Skript mit den entsprechenden Parametern aus der folgenden Tabelle aus.

   - Führen Sie das Skript zuerst im Modus `-dryRun` aus, um eine Vorschau der Migration ohne Änderungen anzuzeigen. Dadurch wird eine Ausgabedatei erzeugt, mit der Sie Probleme identifizieren und beheben können.

- Führen Sie das Skript für die spezifischen Geräterichtlinien aus, die Sie für Tests verwenden möchten. Nach dem Testen und Validieren des 3.x-Agenten können Sie mit dem Skript die Migration auf Ihre Produktionsgeräterichtlinien anwenden.

Parameter	Erforderlich oder optional	Beschreibung
`-copySCExclusions`	Erforderlich	Mit diesem Befehl werden Makroausschlüsse aus der Konfiguration der Skriptsteuerung in die neue Speicherschutz-Konfiguration migriert.

`-allPolicies`
ODER
`-policy '<policy_name>'`
	Erforderlich	`-allPolicies` führt die Migration für alle Geräterichtlinien in Ihrem Mandanten aus.
		`-policy '<policy_name>''` führt die Migration für eine angegebene Geräterichtlinie aus.

`-dryRun`	Optional	Mit diesem Befehl wird eine Vorschau der Skriptausführung angezeigt, ohne Änderungen vorzunehmen. Wenn Sie das Skript in diesem Modus ausführen, wird eine Ausgabedatei in dem Verzeichnis erstellt, aus dem das Skript ausgeführt wird.
`-tenantId '<tenant_ID>'`	Erforderlich	Dieser Befehl gibt die ID des Cylance Endpoint Security-Mandanten an.
`-apiKey '<application_ID>'`	Erforderlich	Dieser Befehl gibt die Anwendungs-ID der Integration an, die Sie unter „Einstellungen > Integrationen“ hinzugefügt haben.
`-apiSecret '<application_secret>`	Erforderlich	Mit diesem Befehl wird der geheime Anwendungsschlüssel der Integration angegeben, die Sie unter „Einstellungen > Integrationen“ hinzugefügt haben.
`-userEmail '<admin_email>'`	Erforderlich	Dieser Befehl gibt die E-Mail-Adresse des Administratorkontos der Cylance-Konsole an, mit dem Sie die Migration ausführen möchten. Das Konto muss über Administratorrechte verfügen.

Parameter	Erforderlich oder optional	Beschreibung
`-region '<region_code>'`	Erforderlich	Dieser Befehl gibt die Region des Cylance Endpoint Security-Mandanten an. Verwenden Sie einen der folgenden Werte: • Nordamerika: `na` (Standardwert, falls nicht angegeben) • Japan: `apne1` • Australien: `au` • Europa: `euc1` • Südamerika: `sae1` • GovCloud: `us`
`-Ignore158xWarning`	Optional	Mit diesem Befehl ignorieren Sie bei der Migration Fehler im Zusammenhang mit der Maximalgröße für Speicherschutz-Ausschlüsse, die von 64 KB bei älteren CylancePROTECT Desktop-Versionen auf 2 MB bei Version 3.x erhöht wurde. **Hinweis:** Verwenden Sie diesen Parameter nur, wenn alle Geräte, die mit der Zielgeräterichtlinie verknüpft sind, Agent 3.x oder höher verwenden.
`-ignore158xCompatibility`	Optional	Dieser Befehl bezieht sich auf einen bestimmten Fehler mit CylancePROTECT Desktop für Windows 2.1.1580 und 1584 (siehe KB 88218). Die Korrektur des Fehlers (Hinzufügen eines zusätzlichen Sternchens (*) zum Platzhalterwert in einem Ausschlusspfad, um den Platzhalter ** zu erhalten) ist standardmäßig in das Skript integriert. Wenn Sie diesen Parameter verwenden, wird die im Skript integrierte Korrektur deaktiviert. **Hinweis:** Verwenden Sie diesen Parameter, wenn die Zielgeräterichtlinie Geräten mit Agent 1578 oder niedriger und Geräten mit Agent 3.x oder höher zugeordnet ist. Verwenden Sie diesen Parameter nicht, wenn die Richtlinie mit Geräten mit Agent 158x verknüpft ist.
`-includeExtensions <extensions>`	Optional	Dieser Befehl gibt die Erweiterungen an, die zur Speicherschutzkonfiguration migriert werden sollen (Beispiel: `-includeExtensions ps1, ja, xlxs`). Wenn Sie diesen Parameter nicht verwenden, werden alle Erweiterungen migriert.

Hinweis: Wenn Sie das Skript im Modus `-dryRun` ausführen, tritt möglicherweise der folgende Fehler in der Ausgabedatei auf: „Entering Modify '<*policy_name*>' Policy... logError : The requested policy has not been converted to MemoryProtection v2.“ Dies kann vorkommen, wenn eine Geräterichtlinie seit einiger

Zeit nicht bearbeitet wurde. Um dieses Problem zu beheben, öffnen und speichern Sie die Richtlinie in der Verwaltungskonsole.

Die PowerShell-Ausgabe zeigt an, ob bestimmte Ausschlüsse für die Skriptsteuerung nicht migriert werden konnten. Sie müssen diese Ausschlüsse manuell zur Speicherschutz-Konfiguration hinzufügen.

Beispiel: Skript im Modus -dryRun ausführen

```
.\sc2memdef_copy.ps1 -copySCExclusions -allPolicies -
dryRun -tenantId '00000000-0000-0000-0000-000000000000' -
apiKey '00000000-0000-0000-0000-000000000000' -apiSecret
 '00000000-0000-0000-0000-000000000000' -userEmail 'user@blackberry.com' -region
 'na'
```

Beispiel: Skript für eine bestimmte Geräterichtlinie ausführen

```
.\sc2memdef_copy.ps1 -copySCExclusions -policy 'userPolicy'
 -tenantId '00000000-0000-0000-0000-000000000000' -
apiKey '00000000-0000-0000-0000-000000000000' -apiSecret
 '00000000-0000-0000-0000-000000000000' -userEmail 'user@blackberry.com' -region
 'na'
```

Beispiel: Skript für alle Geräterichtlinien ausführen

```
.\sc2memdef_copy.ps1 -copySCExclusions -allPolicies -
tenantId '00000000-0000-0000-0000-000000000000' -apiKey
 '00000000-0000-0000-0000-000000000000' -apiSecret
 '00000000-0000-0000-0000-000000000000' -userEmail 'user@blackberry.com' -region
 'na'
```

Wenn Sie fertig sind:

- Prüfen Sie auf der Registerkarte „Speicheraktionen“ der Richtlinien für das Zielgerät die migrierten Ausschlüsse und löschen Sie alle, die nicht für den neuen Verletzungstyp „Gefährliche VBA-Makros“ gelten.
- Löschen Sie die PowerShell-Integration, die Sie der Verwaltungskonsole hinzugefügt haben.

Fehlerbehebung bei CylancePROTECT Desktop 3.x

Windows

Problem	Lösung
Der folgende Fehler wird angezeigt, wenn Sie versuchen, eine Geräterichtlinie nach dem Hinzufügen von Ausschlüssen für den Speicherschutz zu speichern: „Richtlinie konnte nicht gespeichert werden. Bitte versuchen Sie es erneut.“	Wenn der Ausschlusspfad einen Platzhalterwert enthält, der ein einzelnes Sternchen (*) verwendet, ändern Sie den Platzhalter, um ein zusätzliches Sternchen hinzuzufügen, und versuchen Sie dann erneut, die Richtlinie zu speichern. Weitere Informationen finden Sie in KB 94518.
Der CylancePROTECT Desktop 3.0.1000-Agent erstellt eine große Anzahl temporärer Dateien in den temporären Windows-Dateiverzeichnissen.	Führen Sie ein Upgrade auf Agent 3.0.1005 oder höher durch. Weitere Informationen finden Sie in KB 94849.
Eine unerwartete Anzahl von Prozessen wurde nach der Aktualisierung auf CylancePROTECT Desktop 3.x blockiert.	Anleitungen und Best Practices finden Sie in KB 85991.

Linux

Problem	Lösung

Fehlermeldung „Vorgang nicht zulässig“, wenn Sie versuchen, CylancePROTECT-Treiber zu installieren	Einer der folgenden Fehler (oder ein ähnlicher Fehler) wird im Linux-Terminal bei der Installation von CylancePROTECT-Treibern angezeigt:
	`modprobe: ERROR: could not insert 'CyProtectDrvOpen': Operation not permitted`
	`modprobe: ERROR: could not insert 'CyProtectDrv': Operation not permitted`
	`Key was rejected by service`
	Dieser Fehler tritt in der Regel auf, wenn Sie versuchen Linux-Treiber auf einem Gerät zu installieren, auf dem Secure Boot aktiviert ist. Weitere Informationen finden Sie in KB 73487.

Problem	Lösung
Virtualisierungsprobleme	Der CylancePROTECT Desktop-Agent für Linux verwendet die BIOS-Seriennummer und die von dbus erzeugte eindeutige ID (machine-id), um einen Geräte-Fingerabdruck zu erzeugen. In einigen VM-Umgebungen, die ein Golden Image verwenden, können Probleme auftreten. Linux-Maschinen, die aus dem Golden Image generiert werden, können identische BIOS-Seriennummern und von dbus erzeugte IDs beibehalten. Dies kann dazu führen, dass VMs sich bei demselben Gerät auf der Konsole anmelden, anstatt sich als eindeutiges Gerät zu registrieren. Wenn dieses Problem auftritt, wird empfohlen, die BIOS-Seriennummern und Maschinen-IDs der geklonten Maschine zu überprüfen, um sicherzustellen, dass diese Werte für jede Maschine eindeutig sind. Weitere Informationen finden Sie in KB 66123.

macOS

Problem	Lösung

Die Systemerweiterung ist blockiert, wenn der CylancePROTECT Desktop-Agent ausgeführt wird	Nach der Aktualisierung eines CylancePROTECT Desktop-Geräts mit macOS 11.15.0 auf eine neuere macOS-Version tritt der folgende Fehler auf: „Systemerweiterung blockiert. Ein Programm hat versucht, neue Systeme zu laden, die von „Cylance, Inc.“ signiert wurden. Das muss vom Entwickler aktualisiert werden.“
	
	Dieses Problem tritt auf, weil Systemerweiterungen für den CylancePROTECT Desktop-Agenten aktiviert sein müssen. Benutzer müssen zu Systemeinstellungen > Sicherheit und Datenschutz navigieren und dann für die Cylance-Erweiterung auf „Zulassen“ klicken.
	
	Unternehmen, die JAMF zur Bereitstellung von CylancePROTECT Desktop verwenden, müssen Benutzern möglicherweise erlauben, Systemerweiterungen von der JAMF-Konfiguration aus zu genehmigen, indem sie die folgenden Einstellungen verwenden:
	
	• „Benutzern erlauben, Systemerweiterungen zu genehmigen“ aktivieren
	• Unter „Zulässige Team-IDs und Systemerweiterungen“:
	  • Anzeigename: Cylance Protect
	  • Systemerweiterungstypen: Zulässige Systemerweiterungen
	  • Teamkennung: 6ENJ69K633
	  • Zulässige Systemerweiterungen: com.cylance.CylanceEndpointSecurity.extension

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