Cylance Endpoint Security

Guide de mise à niveau de CylancePROTECT Desktop 3.x

Contents

Avantages de la mise à niveau vers CylancePROTECT Desktop 3.x

La version 3.x de CylancePROTECT Desktop représente un grand pas en avant pour le produit, en introduisant de nouvelles fonctionnalités et des améliorations en termes de convivialité pour garantir la sécurité des données et des terminaux de votre organisation.

La mise à niveau vers CylancePROTECT Desktop 3.x vous donne accès aux fonctionnalités suivantes :

Windows

Fonctionnalité	Description
Compatibilité du système d'exploitation	L'agent Windows 3.x ajoute la prise en charge de Windows 11. Pour plus d'informations, consultez la matrice de compatibilité de CylancePROTECT Desktophttps://docs.blackberry.com/en/endpoint-management/compatibility-matrix/blackberry-ues-compatibility-matrix/BlackBerry-Protect-Desktop-agent.
Améliorations de l'agent	• L'agent Windows 3.1 s'exécute en tant que service fiable à l'aide de la technologie AM-PPL (Antimalware Protected Process Light) de Microsoft, qui protège les processus de sécurité de l'agent contre les actions malveillantes. Par exemple, cela permet de protéger l'agent contre la résiliation. Cette fonctionnalité nécessite que le point de terminaison exécute Windows 10 1709 ou versions ultérieures, ou Windows Server 2019 ou versions ultérieures. • L'agent Windows 3.2 envoie à la console de gestion une liste des applications installées sur les terminaux de point de terminaison. Cette fonctionnalité permet aux administrateurs d'identifier les applications installées sur les terminaux de point de terminaison qui peuvent être une source de vulnérabilités, de hiérarchiser les actions contre les vulnérabilités et de les résoudre en conséquence. Les administrateurs peuvent afficher toutes les applications installées sur des points de terminaison enregistrés auprès du locataire et afficher la liste des applications installées sur des points de terminaison individuels. Cette fonctionnalité peut être activée à partir de la stratégie de terminal (paramètres de l'agent).

Fonctionnalité	Description
Améliorations de la protection de la mémoire	• De nouvelles fonctionnalités ont été ajoutées aux types de violation, ce qui entraine la génération d'autres évènements. • Le type de violation « Injection via APC » est disponible dans les paramètres de protection de la mémoire d'une stratégie de terminal. Cette option permet à CylancePROTECT Desktop de détecter un processus qui injecte du code arbitraire dans le processus cible à l'aide d'un appel de procédure asynchrone (APC). Pour plus d'informations, consultez l'article KB 92422. • Le type de violation « Modifications des autorisations de mémoire dans les processus enfants » est disponible dans les paramètres de protection de la mémoire d'une stratégie de terminal. Cette option permet à CylancePROTECT Desktop de détecter lorsqu'un processus en violation a créé un processus enfant et a modifié les autorisations d'accès à la mémoire dans celui-ci. • La convivialité des contrôles de protection de la mémoire a été améliorée. • Amélioration de la détection des violations de lecture LSASS pour les terminaux Windows. • La limite de taille des exclusions de protection de la mémoire est passée de 64 Ko à 2 Mo, ce qui vous permet d'ajouter d'autres exclusions. • Les exclusions relatives aux DLL d'applications tierces sont désormais prises en charge pour permettre l'exécution d'applications tierces avec CylancePROTECT Desktop. Par exemple, si vous exécutez des produits de sécurité tiers outre CylancePROTECT, vous pouvez ajouter une exclusion aux fichiers .dll appropriés afin que CylancePROTECT ignore les violations spécifiques de ces produits. Pour utiliser cette fonctionnalité, vous devez disposer de la version 3.1.1001 ou d'une version ultérieure de l'agent. Pour en savoir plus, consultez la section Paramètre d'exclusion Traiter en tant que DLL dans la stratégie de terminal de protection de la mémoire. • Le capteur de protection de la mémoire pour le type de violation Charge utile malveillante a été amélioré en vue d'optimiser la précision des rapports de violation et de réduire les alertes inutiles. Pour utiliser cette fonctionnalité, vous devez disposer de la version 3.1.1001 ou d'une version ultérieure de l'agent.
Améliorations de la protection	• L'agent Windows 3.1 permet aux administrateurs de définir un intervalle personnalisé pour l'exécution d'une analyse de détection des menaces en arrière-plan à partir de la stratégie de terminal (paramètres de protection). L'intervalle entre les analyses peut être compris entre 1 et 90 jours. L'intervalle entre les analyses par défaut est de 10 jours. Notez que l'augmentation de la fréquence des analyses peut avoir un impact sur les performances du terminal. • L'agent Windows 3.2 permet aux administrateurs de lancer une analyse de détection des menaces en arrière-plan à la demande à partir de la console de gestion. La commande peut être envoyée à partir de l'écran Détails du terminal pour un seul terminal ou à partir de l'écran Terminaux pour plusieurs terminaux à la fois. • La date de la dernière analyse de chaque terminal est consignée dans la console de gestion.

Fonctionnalité	Description
Améliorations du contrôle de script	• Vous pouvez choisir si CylancePROTECT Desktop active ou bloque les alertes Python (2.7, 3.0 à 3.8) et les scripts DLR .NET (par exemple, IronPython). Vous pouvez désactiver le contrôle de script pour ces types de script. • Les scripts VB intégrés qui ont provoqué des évènements de contrôle de script ont été bloqués dans la version 2.1.1580 de l'agent. La détection des violations de contrôle de script VB intégré a été désactivée dans l'agent 3.0.1000 et versions ultérieures. • L'agent Windows 3.1 fonctionne avec l'interface d'analyse de logiciel anti-programmes malveillants (AMSI) de Microsoft. Ainsi, lorsqu'une macro XLM potentiellement dangereuse est exécutée, les informations sur les menaces sont transmises à la console de gestion et l'agent répond à l'interface conformément aux règles de la stratégie de terminal pour les évènements de contrôle de script. Par exemple, l'agent répond s'il faut autoriser ou bloquer l'exécution de la macro. Cette fonctionnalité est activée à partir du paramètre Contrôle des scripts > Macros XLM dans la stratégie de terminal et nécessite que le terminal exécute Windows 10. Assurez-vous de désactiver les macros VBA dans le menu Excel **Fichier > Centre de gestion de la confidentialité > Centre de gestion de la confidentialité Excel > Paramètres des macros**. • L'agent Windows signale les processus parents et d'interpréteur à la console Cylance lorsqu'un script potentiellement malveillant est exécuté. Les administrateurs peuvent ajouter des exclusions au processus parent ou au processus d'interpréteur d'un script afin de permettre son exécution sur un terminal. Pour utiliser cette fonctionnalité, vous devez disposer de la version 3.1.1001 de l'agent. • L'agent Windows 3.2 prend en charge le contrôle de script amélioré à l'aide de l'évaluation des scripts. Les scripts dont l'indice de menace est dangereux ou anormal peuvent être bloqués de manière intelligente et signalés sur la console de gestion. Les administrateurs peuvent configurer les paramètres de contrôle de script dans la stratégie de terminal pour bloquer les scripts que CylancePROTECT considère comme dangereux ou anormaux. • L'agent Windows 3.2 prend en charge le mode Alerte pour les scripts de console PowerShell, afin de signaler les évènements détectés à la console de gestion tout en autorisant leur exécution. Les administrateurs peuvent contrôler le paramètre à partir de l'onglet Contrôle de script dans la stratégie de terminal à l'aide du menu déroulant de la console PowerShell.

Fonctionnalité	Description
Améliorations de la détection des macros	• Dans les stratégies de terminal, la fonctionnalité de détection de macro pour les terminaux Windows a été déplacée de l'onglet Contrôle de script vers l'onglet Actions de mémoire (Exploitation > Macro VBA dangereuse) pour les terminaux exécutant l'agent Windows 2.1.158x ou ultérieure. L'option de contrôle de script précédente de la version 2.1.1578 et des versions antérieures prend en charge les actions d'alerte et de blocage ; la nouvelle option de protection de la mémoire prend en charge les actions Ignorer, Alerter, Bloquer et Terminer. • Vous pouvez désormais ajouter des exclusions pour le type de violation de macro VBA dangereuse dans les paramètres de protection de la mémoire d'une stratégie de terminal. • Les fichiers entraînant des violations de la macro VBA dangereuse s'affichent dans la console de gestion, ce qui vous permet d'identifier les documents fautifs et de déterminer si vous devez les ajouter à la liste d'exclusion.
Améliorations du contrôle du terminal	Vous pouvez désormais autoriser l'accès en lecture seule aux types de périphériques USB suivants : • Image fixe • CD USB / DVD RW • Clé USB • Relais USB VMware • Périphérique portable Windows
Améliorations de la liste de sécurité mondiale	L'ajout d'un hachage SHA256 à la liste de sécurité globale pour les scripts masque désormais tous les évènements de bloc liés à ce hachage dans la console de gestion.
Modifications du journal	Les entrées de journal importantes ont été déplacées du niveau de journal Débogage au niveau de journal Informations.

Linux

Fonctionnalité	Description
Compatibilité du système d'exploitation	L'agent Linux 3.2 prend en charge les distributions Linux suivantes : • Amazon Linux 2023 • Amazon Linux 2, noyau 5.10 L'agent Linux 3.1.x prend en charge les distributions Linux suivantes : • Red Hat Enterprise Linux 9 et 9.1 • Oracle 9 et 9.1 • Oracle UEK 9 et 9.1 • Oracle 8.7 • Oracle UEK 8.7 • SUSE Linux Enterprise Server (SLES) 15 SP4 • Ubuntu 22.04 LTS L'agent Linux 3.0.x prend en charge les distributions Linux suivantes : • Red Hat Enterprise Linux /CentOS 8.4 • Red Hat Enterprise Linux 8.5 • Oracle 8.4 • SUSE (SLES) 12 SP5 • SUSE (SLES) 15 SP2 et SP3 Pour en savoir plus, consultez la matrice de compatibilité de CylancePROTECT Desktop. Pour afficher la liste complète des noyaux et pilotes Linux pris en charge, téléchargez la référence Noyaux Linux pris en charge.
Analyse de détection des menaces en arrière-plan à la demande	Les administrateurs peuvent désormais lancer une analyse de détection des menaces en arrière-plan à la demande à partir de la console de gestion. La commande peut être envoyée à partir de l'écran Détails du terminal pour un seul terminal ou à partir de l'écran Terminaux pour plusieurs terminaux à la fois. Pour utiliser cette fonctionnalité, vous devez disposer de la version 3.2 de l'agent CylancePROTECT Desktop. La date de la dernière analyse de chaque terminal est consignée dans la console de gestion.
Intervalle personnalisé pour l'analyse de détection des menaces en arrière-plan	• Les administrateurs peuvent définir un intervalle personnalisé pour exécuter l'analyse de détection des menaces en arrière-plan à partir de la stratégie de terminal. L'intervalle entre les analyses peut être compris entre 1 et 90 jours. L'intervalle entre les analyses par défaut est de 10 jours. • Pour utiliser cette fonctionnalité, vous devez disposer de la version 3.1 de l'agent CylancePROTECT Desktop. • La date de la dernière analyse de chaque terminal est consignée dans la console de gestion.

Fonctionnalité	Description
Mise à jour automatique du pilote Linux	• L'agent CylancePROTECT Desktop 3.1.1000 pour les terminaux Linux peut désormais solliciter une mise à jour vers le dernier pilote d'agent pris en charge lorsqu'un noyau mis à jour est détecté sur le système. Par exemple, si le noyau Linux est mis à jour et que le pilote de l'agent actuellement installé ne le prend pas en charge, l'agent peut dorénavant mettre à jour automatiquement le pilote dès qu'un pilote compatible est disponible. • Pour utiliser cette fonctionnalité, vous devez disposer de l'agent CylancePROTECT Desktop 3.1.1000 et de la version 3.1.1000 ou ultérieure du pilote de l'agent. • Pour activer cette fonctionnalité, sélectionnez l'option de mise à jour automatique du pilote Linux dans la règle de mise à jour basée sur la zone dans le menu Paramètres > Mettre à jour de la console de gestion.
Améliorations de la protection de la mémoire	• De nouvelles fonctionnalités ont été ajoutées aux types de violation, ce qui entraine la génération d'autres évènements. • La convivialité des contrôles de protection de la mémoire a été améliorée. • La limite de taille des exclusions de protection de la mémoire est passée de 64 Ko à 2 Mo, ce qui vous permet d'ajouter d'autres exclusions.

macOS

Fonctionnalité	Description
Compatibilité du système d'exploitation	• L'agent CylancePROTECT Desktop 3.2.x ajoute la prise en charge de macOS 14 (Sonoma). • L'agent CylancePROTECT Desktop 3.1.x ajoute la prise en charge de macOS 13 (Ventura). • L'agent CylancePROTECT Desktop 3.0.x ajoute la prise en charge de macOS 12 (Monterey).
Contrôle du terminal USB	L'agent CylancePROTECT Desktop pour macOS 3.3 prend en charge la fonction de contrôle de terminal USB, qui permet aux administrateurs de contrôler s'ils autorisent ou bloquent l'accès aux terminaux de stockage de masse USB. Les administrateurs peuvent activer le contrôle des terminaux macOS à partir de la stratégie de terminal pour les terminaux de stockage classés comme lecteurs optiques USB ou lecteurs de stockage USB (tels que les disques durs ou les lecteurs flash).
Analyse de détection des menaces en arrière-plan à la demande	Les administrateurs peuvent désormais lancer une analyse de détection des menaces en arrière-plan à la demande à partir de la console de gestion. La commande peut être envoyée à partir de l'écran Détails du terminal pour un seul terminal ou à partir de l'écran Terminaux pour plusieurs terminaux à la fois. Pour utiliser cette fonctionnalité, vous devez disposer de la version 3.2 de l'agent CylancePROTECT Desktop. La date de la dernière analyse de chaque terminal est consignée dans la console de gestion.

Fonctionnalité	Description
Intervalle personnalisé pour l'analyse de détection des menaces en arrière-plan	• Les administrateurs peuvent définir un intervalle personnalisé pour exécuter l'analyse de détection des menaces en arrière-plan à partir de la stratégie de terminal. L'intervalle entre les analyses peut être compris entre 1 et 90 jours. L'intervalle entre les analyses par défaut est de 10 jours. • La date de la dernière analyse de chaque terminal est consignée dans la console de gestion.
Améliorations de la protection de la mémoire	• De nouvelles fonctionnalités ont été ajoutées aux types de violation, ce qui entraine la génération d'autres évènements. • La convivialité des contrôles de protection de la mémoire a été améliorée. • La limite de taille des exclusions de protection de la mémoire est passée de 64 Ko à 2 Mo, ce qui vous permet d'ajouter d'autres exclusions.

Pour plus d'informations sur les fonctionnalités supplémentaires des derniers agents 3.x, ainsi qu'une liste complète des problèmes résolus, consultez les Notes de mise à jour de Cylance Endpoint Security.

Pour bénéficier de ces améliorations et des améliorations à venir dans les futures versions de CylancePROTECT Desktop, BlackBerry recommande vivement de mettre à niveau tous les terminaux avec l'agent 2.x.158x ou une version antérieure vers la dernière version de l'agent 3.x. Ce guide traite des considérations et des instructions supplémentaires pour une mise à niveau réussie.

Mise à niveau vers CylancePROTECT Desktop 3.x

Cette section fournit des conseils détaillés et des pratiques recommandées pour garantir la réussite de la mise à niveau vers CylancePROTECT Desktop version 3.x.

Étape	Action
1	Consultez les conseils pour préparer votre environnement de test.
2	Examinez les chemins de mise à niveau de l'agent pour déterminer le chemin spécifique que vous devez suivre.
3	Configuration et test de la protection de la mémoire.
4	Configurer et tester la détection des macros (Windows uniquement).
5	Si nécessaire, migrez les exclusions de macro de contrôle de script vers la nouvelle configuration de protection de la mémoire.
6	Une fois les tests et la validation terminés dans l'environnement de test, appliquez la mise à niveau et les stratégies de terminal mises à jour à votre environnement de production.

Préparation de votre environnement test

- BlackBerry recommande de tester la mise à niveau vers CylancePROTECT Desktop pour Windows 3.x dans une zone de test dédiée avant de déployer la mise à niveau dans votre environnement de production. Pour plus d'informations sur les zones, consultez la section Configuration des zones dans le contenu relatif à la configuration de Cylance Endpoint Security.
- Configurez vos terminaux de test avec les applications et les configurations qui représentent précisément votre environnement de production.
- Créez des stratégies de terminaux dédiées que vous utiliserez pour vos zones et terminaux de test. Vous pouvez créer de nouvelles stratégies de terminal ou copier et modifier des stratégies existantes.
- Configurez les règles de mise à jour basées sur les zones dans la console de gestion pour limiter la mise à niveau vers la version 3.x aux zones et aux terminaux dédiés que vous prévoyez d'utiliser pour les tests. Pour obtenir des instructions, consultez la section Gestion des mises à jour pour les agents CylancePROTECT Desktop et CylanceOPTICS dans le contenu de la configuration de Cylance Endpoint Security.
- BlackBerry recommande de télécharger l'outil Support Collection à partir de l'article KB 66596. Si vous contactez l'assistance BlackBerry pour obtenir de l'aide, l'assistance peut vous demander d'exécuter l'outil afin de recueillir des données supplémentaires.
- Consultez les chemins de mise à niveau de l'agent pour déterminer le chemin spécifique que vous devez suivre.
- Après avoir terminé les activités de configuration et de test de ce guide et validé la mise à niveau dans vos zones de test, vous pouvez appliquer la mise à niveau de l'agent et les stratégies de terminal mises à jour à votre environnement de production.

Chemins de mise à niveau de l'agent CylancePROTECT Desktop 3.x

Les chemins de mise à niveau suivants ont été testés et sont officiellement pris en charge :

Chemin de mise à niveau vers l'agent Windows version 3.x

Version de l'agent actuelle	Chemin de mise à niveau
2.0.154x	→ 2.1.157x → 3.2.1000
2.1.156x	→ 2.1.157x → 3.2.1000
2.1.157x	→ 3.2.1000
2.1.158x	→ 3.2.1000
3.0	→ 3.2.1000
3.1	→ 3.2.1000

Chemin de mise à niveau vers l'agent Linux version 3.x

Version de l'agent actuelle	Chemin de mise à niveau
2.1.157x ou version antérieure	→ 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

Chemin de mise à niveau vers l'agent macOS version 3.x

Version de l'agent actuelle	Chemin de mise à niveau
2.1.156x	→ 2.1.158x → 3.3.1000
2.1.158x	→ 3.3.1000
2.1.159x	→ 3.3.1000
3.0	→ 3.3.1000
3.1	→ 3.3.1000

Version de l'agent actuelle	Chemin de mise à niveau
3.2	→ 3.3.1000

Configuration et test de la protection de la mémoire

CylancePROTECT Desktop 3.x introduit diverses améliorations de protection de la mémoire et une meilleure visibilité sur l'activité des applications et des processus sur un terminal. Dans certaines situations, les applications effectuent des opérations qui peuvent être considérées comme malveillantes, mais qui sont effectuées à des fins légitimes. BlackBerry recommande de suivre les étapes et les bonnes pratiques ci-dessous pour garantir le bon réglage de l'agent CylancePROTECT Desktop 3.x avant de le déployer dans votre environnement de production. Pour plus d'informations sur les types de violation de protection de la mémoire, consultez la section Protection de la mémoire dans le contenu relatif à la configuration Cylance Endpoint Security.

1. Dans la barre de menus de la console de gestion, cliquez sur **Stratégies > Stratégie de terminal**.
2. Cliquez sur la stratégie de terminal pour vos terminaux de test.
3. Dans l'onglet **Actions de mémoire**, cochez la case **Protection de la mémoire**.
4. Dans le tableau **Type de violation**, développez **Exploitation**, **Injection de processus** et **Escalade**. Pour tous les types de violation répertoriés sous **Disponible pour la version 2.1.1580 de et les versions ultérieures** et **Disponible pour CylancePROTECT 3.0 et les versions ultérieures**, sélectionnez l'action **ALERTER**.
5. Enregistrez la stratégie de terminal.
6. Exécutez CylancePROTECT Desktop 3.x sur vos terminaux de test et consultez les alertes afin de déterminer le risque de ces exploitations pour votre environnement. Si l'une de ces alertes présente un risque faible et a un impact sur l'activité, vous pouvez ajouter des exclusions ciblées de protection de la mémoire. Pour obtenir des instructions et des conseils, consultez la section Protection de la mémoire.

   Il est recommandé de redémarrer chaque terminal de test après l'installation ou la mise à niveau vers CylancePROTECT Desktop 3.x.

À la fin : Après avoir examiné les alertes et ajouté les exclusions nécessaires, vous pouvez modifier les actions de type de violation dans la stratégie de terminal selon vos besoins (par exemple, Bloquer ou Terminer).

Configurer et tester la détection des macros (Windows uniquement)

Deux options sont disponibles dans une stratégie de terminal pour détecter et répondre aux macros potentiellement dangereuses sur les terminaux Windows. L'option Macros de l'onglet Contrôle de script s'applique à l'agent Windows 2.1.1578 et versions antérieures. La nouvelle option Exploitation > Macro VBA dangereuse de l'onglet Actions de mémoire s'applique à l'agent Windows 2.1.1580 et versions ultérieures. Lorsque vous testez votre mise à niveau vers l'agent 3.x, vous devez vérifier votre configuration actuelle pour détecter et répondre aux macros, mais aussi configurer la nouvelle option de macro VBA dangereuse en conséquence.

1. Dans la barre de menus de la console de gestion, cliquez sur **Stratégies > Stratégie de terminal**.
2. Cliquez sur votre stratégie de terminal de production.
3. Dans l'onglet **Contrôle de script**, notez la configuration actuelle des macros (Alerter ou Bloquer).
4. Dans **Stratégies > Stratégie de terminal**, cliquez sur la stratégie de terminal pour vos terminaux de test.
5. Dans l'onglet **Actions de mémoire**, développez **Exploitation**.
6. Pour le type de violation **Macro VBA dangereuse**, définissez l'action appropriée (Ignorer, Alerter, Bloquer ou Terminer).
7. Enregistrez la stratégie de terminal.

8. Si nécessaire, migrez les exclusions de macro de contrôle de script vers la nouvelle configuration de protection de la mémoire.
9. Exécutez CylancePROTECT Desktop 3.x sur les terminaux de test qui utilisent des fichiers avec des macros couramment utilisées dans votre organisation. Si nécessaire, ajoutez des exclusions de protection de la mémoire supplémentaires pour les macros sécurisées. Pour obtenir des instructions et des conseils, consultez la section Protection de la mémoire dans le contenu relatif à la configuration Cylance Endpoint Security.

Migrer les exclusions de macro de contrôle de script vers la nouvelle configuration de protection de la mémoire (Windows uniquement)

Si vous avez précédemment ajouté des exclusions de macro dans l'onglet Contrôle de script de vos stratégies de terminal, vous devez migrer ces exclusions vers la nouvelle configuration de protection de la mémoire pour CylancePROTECT Desktop Windows 3.x. Si vous souhaitez migrer manuellement les exclusions de contrôle de script, il vous suffit d'enregistrer les exclusions que vous avez ajoutées dans l'onglet Contrôle de script de vos stratégies de terminal, puis d'ajouter les mêmes exclusions dans l'onglet Actions de mémoire de vos stratégies de terminal.

Suivez les étapes ci-dessous si vous souhaitez migrer les exclusions de contrôle de script existantes à l'aide d'un script PowerShell fourni par BlackBerry.

Remarque : Les étapes ci-dessous s'appliquent aux locataires gérés à l'aide de la console Cylance. Si vous gérez des locataires à l'aide de la Console multilocataire, consultez l' article KB 92149.

Avant de commencer :

- Vérifiez que PowerShell est installé sur votre ordinateur et que les scripts PowerShell ne sont pas bloqués par le logiciel de sécurité, y compris CylancePROTECT Desktop. Si CylancePROTECT Desktop est installé sur votre ordinateur, dans la stratégie attribuée à votre terminal, vérifiez que **Contrôle de script > Bloquer l'utilisation de la console PowerShell** est désactivé.
- Dans la console Cylance, ajoutez une intégration avec les privilèges d'API suivants et enregistrez l'ID et le code secret d'application obtenus :
  - **Stratégies** : lecture, modification
  - **Utilisateurs** : lecture
- Dans **Paramètres > Intégrations**, enregistrez l'**ID de locataire**.
- Lorsque vous exécutez le script, spécifiez l'adresse e-mail d'un compte administrateur de la console Cylance. Vérifiez que le compte que vous souhaitez utiliser a le rôle Administrateur.
- Dans les stratégies de terminal où vous souhaitez migrer les exclusions du contrôle de script vers la protection de la mémoire, vérifiez que le contrôle de script est activé et que les exclusions de macro sont présentes.
  - Le script ignorera les stratégies pour lesquelles le contrôle de script est désactivé et les stratégies qui ne comportent pas d'exclusions de contrôle de script.
  - Le script ne migre pas les listes d'exclusion contenant des caractères multioctets. Vous devez ajouter ces exclusions manuellement.
- Téléchargez le script PowerShell.

1. Ouvrez une invite de commande PowerShell et remplacez le répertoire par l'emplacement du script.
2. Exécutez le script en utilisant les paramètres appropriés du tableau ci-dessous.

   - Commencez par exécuter le script en mode `-dryRun` pour prévisualiser la migration sans apporter de modifications. Cela génère un fichier de sortie que vous pouvez utiliser pour identifier et corriger les problèmes.
   - Exécutez le script pour les stratégies de terminal spécifiques que vous prévoyez d'utiliser pour les tests. Après avoir testé et validé l'agent 3.x, vous pouvez utiliser le script pour appliquer la migration à vos stratégies de terminal de production.

Paramètre	Obligatoire ou facultative	Description
`-copySCExclusions`	Requis	Cette commande exécute la migration des exclusions de macro de la configuration de contrôle de script vers la nouvelle configuration de protection de la mémoire.

`-allPolicies`
OU
`-policy '<policy_name>'`
	Requis	`-allPolicies` exécute la migration de toutes les stratégies de terminal de votre locataire.
		`-policy '<policy_name>''` exécute la migration d'une stratégie de terminal spécifique.

`-dryRun`	Facultative	Cette commande affiche un aperçu de l'exécution du script sans apporter de modifications. Lorsque vous exécutez le script dans ce mode, il crée un fichier de sortie dans le répertoire à partir duquel le script est exécuté.
`-tenantId '<tenant_ID>'`	Requis	Cette commande spécifie l'ID de votre locataire Cylance Endpoint Security.
`-apiKey '<application_ID>'`	Requis	Cette commande spécifie l'ID d'application de l'intégration que vous avez ajoutée dans Paramètres > Intégrations.
`-apiSecret '<application_secret>`	Requis	Cette commande spécifie le secret d'application de l'intégration que vous avez ajoutée dans Paramètres > Intégrations.
`-userEmail '<admin_email>'`	Requis	Cette commande spécifie l'adresse e-mail du compte administrateur de la console Cylance que vous souhaitez utiliser pour exécuter la migration. Le compte doit avoir le rôle Administrateur.
`-region '<region_code>'`	Requis	Cette commande spécifie la région de votre locataire Cylance Endpoint Security. Utilisez une des valeurs suivantes : • Amérique du Nord : `na` (valeur par défaut si ce champ n'est pas spécifié) • Japon : `apne1` • Australie : `au` • Europe : `euc1` • Amérique du Sud : `sae1` • GovCloud : `us`

Paramètre	Obligatoire ou facultative	Description
`-Ignore158xWarning`	Facultative	Cette commande permet au processus de migration d'ignorer les erreurs liées à la limite de taille des exclusions de protection de la mémoire, qui est passée de 64 Ko pour les versions antérieures de CylancePROTECT Desktop à 2 Mo pour la version 3.x. **Remarque :** Utilisez ce paramètre uniquement si tous les terminaux associés à la stratégie de terminal cible utilisent l'agent de version 3.x ou versions ultérieures.
`-ignore158xCompatibility`	Facultative	Cette commande est liée à un défaut spécifique de CylancePROTECT Desktop sur Windows 2.1.1580 et 1584 (consulter l' article KB 88218). La correction du défaut (en ajoutant un astérisque (*) supplémentaire à la valeur du caractère générique dans un chemin d'exclusion pour faire du caractère générique **) est intégrée au script par défaut. Si vous utilisez ce paramètre, la correction intégrée au script est désactivée. **Remarque :** Utilisez ce paramètre si la stratégie de terminal cible est associée à des terminaux avec l'agent 1578 ou versions antérieures et à des terminaux avec l'agent 3.x ou versions ultérieures. Si la stratégie est associée à des terminaux avec l'agent 158x, n'utilisez pas ce paramètre.
`-includeExtensions <extensions>`	Facultative	Cette commande spécifie les extensions à migrer vers la configuration de protection de la mémoire (par exemple, `-includeExtensions ps1, ja, xlxs`). Si vous n'utilisez pas ce paramètre, toutes les extensions sont migrées.

Remarque : Lorsque vous exécutez le script en mode `-dryRun`, l'erreur suivante peut se produire dans le fichier de sortie : « Accès à la modification '*<policy_name>*' Stratégie... logError : la stratégie demandée n'a pas été convertie en Memoryprotection v2 ». Cette erreur peut survenir si une stratégie de terminal n'a pas été modifiée depuis un certain temps. Pour résoudre ce problème, ouvrez et enregistrez la stratégie dans la console de gestion.

La sortie PowerShell indique si des exclusions de contrôle de script n'ont pas pu être migrées. Vous devez ajouter manuellement ces exclusions à la configuration de protection de la mémoire.

Exemple : exécutez le script en mode -dryRun

```
.\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'
```

Exemple : exécutez le script pour une stratégie de terminal spécifique

```
.\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'
```

Exemple : exécutez le script pour toutes les stratégies de terminal

```
.\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'
```

À la fin :

- Sous l'onglet Actions de mémoire des stratégies de terminal cible, vérifiez les exclusions migrées et supprimez celles qui ne s'appliquent pas au nouveau type de violation de macro VBA dangereux.
- Supprimez l'intégration PowerShell que vous avez ajoutée à la console de gestion.

Résolution des problèmes liés à CylancePROTECT Desktop 3.x

Windows

Problème	Solution
L'erreur suivante s'affiche lorsque vous essayez d'enregistrer une stratégie de terminal après avoir ajouté des exclusions de protection de la mémoire : « Impossible d'enregistrer la stratégie. Veuillez réessayer. ».	Si le chemin d'exclusion inclut une valeur de caractère générique qui utilise un seul astérisque (*), modifiez le caractère générique pour ajouter un astérisque supplémentaire (**), puis réessayez d'enregistrer la règle. Pour plus d'informations, consultez KB 94518.
L'agent CylancePROTECT Desktop 3.0.1000 crée un grand nombre de fichiers temporaires dans les répertoires de fichiers temporaires Windows.	Mettre à niveau l'agent vers la version 3.0.1000 ou versions ultérieures. Pour plus d'informations, consultez KB 94849.
Un nombre inattendu de processus est bloqué après la mise à niveau vers CylancePROTECT Desktop 3.x.	Pour obtenir des conseils et des bonnes pratiques, consultez l'article KB 85991.

Linux

Problème	Solution

Erreurs « Opération non autorisée » lorsque vous tentez d'installer les pilotes CylancePROTECT	L'une des erreurs suivantes (ou une erreur similaire) s'affiche sur le terminal Linux lorsque vous installez les pilotes CylancePROTECT :
	`modprobe: ERROR: could not insert 'CyProtectDrvOpen': Operation not permitted`
	`modprobe: ERROR: could not insert 'CyProtectDrv': Operation not permitted`
	`Key was rejected by service`
	Cette erreur se produit généralement lorsque vous tentez d'installer les pilotes Linux sur un terminal sur lequel le démarrage sécurisé est activé. Pour en savoir plus, consultez l'article 73487 de la base de connaissances.

Problème	Solution
Problèmes de virtualisation	L'agent CylancePROTECT Desktop pour Linux utilise le numéro de série du BIOS et l'ID unique généré par dbus (machine-id) pour générer une empreinte de terminal. Des problèmes peuvent survenir dans certains environnements de VM ayant recours à une image de référence. Les machines Linux générées à partir de l'image de référence peuvent conserver les mêmes numéros de série du BIOS et les ID générés par dbus. Cela peut entrainer l'enregistrement des machines virtuelles dans le même terminal sur la console au lieu de l'enregistrement en tant que terminal unique. Si ce problème se produit, il est recommandé de vérifier les numéros de série du BIOS et les machine-id de la machine clonée pour vous assurer que ces valeurs sont uniques pour chaque machine. Pour en savoir plus, consultez l'article 66123 de la base de connaissance.

macOS

Problème	Solution

L'extension système est bloquée lors de l'exécution de l'agent CylancePROTECT Desktop	Après la mise à niveau d'un terminal CylancePROTECT Desktop avec macOS 11.15.0 vers une version ultérieure de macOS, l'erreur suivante se produit : « Extension système bloquée. Un programme a tenté de charger un ou plusieurs nouveaux systèmes signés par « Cylance, Inc. » Le développeur doit effectuer une mise à jour. »
	
	Ce problème se produit, car les extensions système doivent être activées pour l'agent CylancePROTECT Desktop. Les utilisateurs doivent accéder à Préférences système > Sécurité et confidentialité, puis cliquer sur Autoriser en regard de l'extension Cylance.
	
	Il est possible que les organisations ayant recours à JAMF pour le déploiement de CylancePROTECT Desktop doivent autoriser les utilisateurs à approuver les extensions système au sein de la configuration JAMF, en utilisant les paramètres suivants :
	
	• Activez l'option Autoriser les utilisateurs à approuver les extensions système.
	• Sous ID d'équipe et extensions système autorisés :
	  • Nom affiché : Cylance Protect
	  • Types d'extension système : extensions système autorisées
	  • Identifiant de l'équipe : 6ENJ69K633
	  • Extensions système autorisées : com.cylance.CylanceEndpointSecurity.extension

Informations juridiques

Cette documentation, y compris la documentation incluse pour référence telle que celle fournie ou mise à disposition sur le site Web BlackBerry, est fournie ou mise à disposition « EN L'ÉTAT » et « TELLE QUELLE », sans condition ni garantie en tout genre de la part de BlackBerry Limited et de ses filiales (« BlackBerry »), et BlackBerry décline toute responsabilité en cas d'erreur ou d'oubli typographique, technique ou autre inexactitude contenue dans ce document. Pour des raisons de protection des informations confidentielles et/ou des secrets commerciaux de BlackBerry, cette documentation peut décrire certains aspects de la technologie BlackBerry en termes généraux. BlackBerry se réserve le droit de modifier périodiquement les informations contenues dans cette documentation. Cependant, BlackBerry ne s'engage en aucune manière à vous communiquer les modifications, mises à jour, améliorations ou autres ajouts apportés à cette documentation.

La présente documentation peut contenir des références à des sources d'informations, du matériel ou des logiciels, des produits ou des services tiers, y compris des composants et du contenu tel que du contenu protégé par copyright et/ou des sites Web tiers (ci-après dénommés collectivement « Produits et Services tiers »). BlackBerry ne contrôle pas et décline toute responsabilité concernant les Produits et Services tiers, y compris, sans s'y limiter, le contenu, la précision, le respect du code de la propriété intellectuelle, la compatibilité, les performances, la fiabilité, la légalité, l'éthique, les liens ou tout autre aspect desdits Produits et Services tiers. La présence d'une référence aux Produits et Services tiers dans cette documentation ne suppose aucunement que BlackBerry se porte garant des Produits et Services tiers ou de la tierce partie concernée.

SAUF DANS LA MESURE SPÉCIFIQUEMENT INTERDITE PAR LES LOIS EN VIGUEUR DANS VOTRE JURIDICTION, TOUTES LES CONDITIONS, GARANTIES OU REPRÉSENTATIONS DE TOUTE NATURE, EXPRESSES OU TACITES, NOTAMMENT (SANS LIMITATIONS) LES CONDITIONS, GARANTIES OU REPRÉSENTATIONS DE DURABILITÉ, D'ADÉQUATION À UNE UTILISATION OU À UN BUT PARTICULIER, DE COMMERCIALISATION, DE QUALITÉ MARCHANDE, DE NON-INFRACTION, DE SATISFACTION DE LA QUALITÉ OU DE TITRE, OU RÉSULTANT D'UNE LOI, D'UNE COUTUME, D'UNE PRATIQUE OU D'UN USAGE COMMERCIAL, OU EN RELATION AVEC LA DOCUMENTATION OU SON UTILISATION, OU LA PERFORMANCE OU NON-PERFORMANCE DES LOGICIELS, DU MATÉRIEL, DES SERVICE OU DES PRODUITS ET SERVICES TIERS CITÉS, SONT EXCLUES. VOUS POUVEZ JOUIR D'AUTRES DROITS QUI VARIENT SELON L'ÉTAT OU LA PROVINCE. CERTAINES JURIDICTIONS N'AUTORISENT PAS L'EXCLUSION OU LA LIMITATION DES GARANTIES ET CONDITIONS IMPLICITES. DANS LA MESURE AUTORISÉE PAR LES LOIS, TOUTE GARANTIE OU CONDITION IMPLICITE RELATIVE À LA DOCUMENTATION, DANS LA MESURE OÙ ELLES NE PEUVENT PAS ÊTRE EXCLUES EN VERTU DES CLAUSES PRÉCÉDENTES, MAIS PEUVENT ÊTRE LIMITÉES, SONT PAR LES PRÉSENTES LIMITÉES À QUATRE-VINGT-DIX (90) JOURS À COMPTER DE LA DATE DE LA PREMIÈRE ACQUISITION DE LA DOCUMENTATION OU DE L'ARTICLE QUI FAIT L'OBJET D'UNE RÉCLAMATION.

DANS LA MESURE MAXIMALE PERMISE PAR LES LOIS EN VIGUEUR DANS VOTRE JURIDICTION, EN AUCUN CAS BLACKBERRY N'EST RESPONSABLE DES DOMMAGES LIÉS À LA PRÉSENTE DOCUMENTATION OU À SON UTILISATION, OU À LA PERFORMANCE OU NON-PERFORMANCE DES LOGICIELS, DU MATÉRIEL, DES SERVICES OU DES PRODUITS ET SERVICES TIERS MENTIONNÉS DANS LES PRÉSENTES, ET NOTAMMENT, SANS S'Y LIMITER, DES DOMMAGES DIRECTS, EXEMPLAIRES, ACCIDENTELS, INDIRECTS, SPÉCIAUX, PUNITIFS OU AGGRAVÉS, DES DOMMAGES LIÉS À UNE PERTE DE PROFITS OU DE REVENUS, UN MANQUE À GAGNER, UNE INTERRUPTION D'ACTIVITÉ, UNE PERTE D'INFORMATIONS COMMERCIALES, UNE PERTE D'OPPORTUNITÉS COMMERCIALES, LA CORRUPTION OU LA PERTE DE DONNÉES, LE NON-ENVOI OU LA NON-RÉCEPTION DE DONNÉES, DES PROBLÈMES LIÉS À DES APPLICATIONS UTILISÉES AVEC DES PRODUITS OU SERVICES BLACKBERRY, DES COUTS D'INDISPONIBILITÉ, LA PERTE D'UTILISATION DES PRODUITS OU SERVICES BLACKBERRY EN TOUT OU EN PARTIE, OU DE TOUT SERVICE DE COMMUNICATION, DU COUT DE BIENS DE

SUBSTITUTION, DES FRAIS DE GARANTIE, DES ÉQUIPEMENTS OU SERVICES, DES COUTS DE CAPITAL, OU AUTRES PERTES FINANCIÈRES SIMILAIRES, PRÉVISIBLES OU NON, MÊME SI BLACKBERRY A ÉTÉ INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES.

DANS LA MESURE MAXIMALE PERMISE PAR LES LOIS APPLICABLES DANS VOTRE JURIDICTION, BLACKBERRY N'EST NULLEMENT TENU PAR DES OBLIGATIONS, DEVOIRS OU RESPONSABILITÉS, CONTRACTUELS, DÉLICTUELS OU AUTRES, PAS MÊME PAR UNE RESPONSABILITÉ EN CAS DE NÉGLIGENCE OU RESPONSABILITÉ STRICTE ET NE VOUS EST REDEVABLE EN RIEN.

LES LIMITATIONS, EXCLUSIONS ET CLAUSES DE NON-RESPONSABILITÉ CONTENUES DANS LES PRÉSENTES S'APPLIQUENT : (A) INDÉPENDAMMENT DE LA NATURE DE LA CAUSE D'ACTION, DE DEMANDE OU D'ACTION ENTREPRISE PAR VOUS, NOTAMMENT, SANS S'Y LIMITER, POUR RUPTURE DE CONTRAT, NÉGLIGENCE, FAUTE, RESPONSABILITÉ STRICTE OU TOUTE AUTRE THÉORIE LÉGALE, ET RESTENT APPLICABLES EN CAS DE RUPTURES SUBSTANTIELLES OU DE MANQUEMENT AU BUT ESSENTIEL DU PRÉSENT CONTRAT OU DE TOUT RECOURS ENVISAGEABLE PAR LES PRÉSENTES ; ET (B) À BLACKBERRY ET À SES FILIALES, LEURS AYANTS DROIT, REPRÉSENTANTS, AGENTS, FOURNISSEURS (NOTAMMENT LES FOURNISSEURS DE SERVICES), REVENDEURS AGRÉÉS BLACKBERRY (NOTAMMENT LES FOURNISSEURS DE SERVICES) ET LEURS DIRECTEURS, EMPLOYÉS ET SOUS-TRAITANTS RESPECTIFS.

OUTRE LES LIMITATIONS ET EXCLUSIONS SUSMENTIONNÉES, EN AUCUN CAS, LES DIRECTEURS, EMPLOYÉS, AGENTS, REVENDEURS, FOURNISSEURS, SOUS-TRAITANTS DE BLACKBERRY OU DE SES FILIALES N'ONT UNE RESPONSABILITÉ CONSÉCUTIVE OU RELATIVE À LA PRÉSENTE DOCUMENTATION.

Avant de vous abonner, d'installer ou d'utiliser des Produits et Services tiers, il est de votre responsabilité de vérifier que votre fournisseur de services prend en charge toutes les fonctionnalités. Certains fournisseurs de services peuvent ne pas proposer de fonctionnalités de navigation Internet avec un abonnement à BlackBerry® Internet Service. Vérifiez auprès de votre fournisseur de services la disponibilité, les accords d'itinérance, les plans de service et les fonctionnalités. L'installation ou l'utilisation de Produits et Services tiers avec des produits et services BlackBerry peuvent nécessiter un ou plusieurs brevets, marques commerciales, licences de copyright ou autres licences à des fins de protection des droits d'autrui. Vous êtes seul responsable de votre décision d'utiliser ou non les Produits et Services tiers et si cela nécessite l'obtention de licences tierces. Si de telles licences sont requises, vous êtes seul responsable de leur acquisition. Vous ne devez pas installer ou utiliser de Produits et Services tiers avant d'avoir acquis la totalité des licences nécessaires. Les Produits et Services tiers fournis avec les produits et services BlackBerry vous sont fournis à toutes fins utiles « EN L'ÉTAT » sans conditions, garanties ou représentations expresses ou tacites d'aucune sorte par BlackBerry, et BlackBerry n'engage aucune responsabilité sur les Produits et Services tiers à cet égard. L'utilisation que vous faites des Produits et Services tiers est régie par et dépendante de votre acceptation des termes des licences et autres accords distincts applicables à cet égard avec d'autres parties, sauf dans la limite couverte expressément par une licence ou autre accord conclu avec BlackBerry.

Les conditions d'utilisation de tout produit ou service BlackBerry sont stipulées dans une licence ou autre accord distinct conclu avec BlackBerry à cet égard. LE CONTENU DE CETTE DOCUMENTATION N'EST PAS DESTINÉ À REMPLACER LES ACCORDS OU GARANTIES EXPRÈS ET ÉCRITS FOURNIS PAR BLACKBERRY POUR UNE PARTIE DES PRODUITS OU SERVICES BLACKBERRY AUTRES QUE CETTE DOCUMENTATION.

BlackBerry Enterprise Software incorpore des éléments logiciels tiers. La licence et les informations de copyright associées à ce logiciel sont disponibles à l'adresse http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue Est
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,

Maidenhead, Berkshire SL6 1RL
Royaume-Uni

Publié au Canada