Cylance Endpoint Security

Présentation et architecture

Contents

Qu'est-ce que Cylance Endpoint Security ?

Cylance Endpoint Security offre une solution de sécurité unifiée pour les points de terminaison qui est conçue pour la nouvelle réalité. Il consolide les meilleurs outils basés sur l'IA disponibles pour détecter, protéger et corriger les menaces sur chaque point de terminaison. Aujourd'hui, les cybercriminels utilisent l'intelligence artificielle (IA) pour créer des menaces de plus en plus avancées qui optimisent la portée et l'impact de leurs attaques. Aujourd'hui, les solutions de la gamme de produits doivent également tirer parti de la puissance de l'apprentissage automatique et de l'IA. Cylance Endpoint Security fournit une solution basée sur l'IA pour Zero Trust sur l'ensemble des terminaux, des réseaux, des applications et des personnes.

L'approche Zero Trust modernise la sécurité du réseau tout en améliorant l'expérience réseau pour les utilisateurs finaux. Par défaut, le modèle de sécurité Zero Trust ne fait confiance à personne, y compris aux utilisateurs du réseau professionnel. Chaque utilisateur, point de terminaison et réseau est supposé être potentiellement hostile. Dans le cadre du modèle de sécurité Zero Trsut, aucun utilisateur ne peut accéder à quoi que ce soit tant qu'il n'a pas prouvé son identité, que son accès est autorisé, que le réseau auquel il est connecté n'est pas compromis et qu'il n'agit pas de manière malveillante, ou qu'un logiciel malveillant se cache sur son appareil.

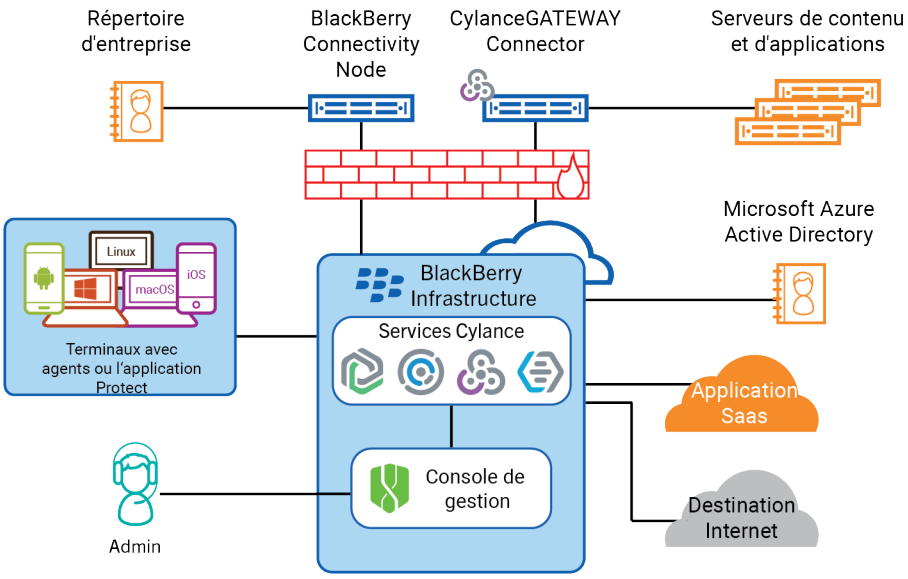
Principales fonctionnalités de Cylance Endpoint Security

Cylance Endpoint Security offre un large éventail de capacités de sécurité grâce à plusieurs fonctionnalités interconnectées :

Fonctionnalité	Description
Détection et blocage des ransomware, des logiciels malveillants et autres menaces	CylancePROTECT Desktop bloque les ransomwares et autres programmes malveillants sur les terminaux Windows, macOS et Linux à l'aide d'une approche mathématique de l'identification des programmes malveillants. Cette fonctionnalité utilise des techniques d'apprentissage automatique au lieu de signatures réactives, de systèmes basés sur la confiance ou de bacs à sable pour fournir une détection et une réponse des points de terminaison qui rendent inutiles les nouveaux ransomware, logiciels malveillants, virus, bots et variantes futures. CylancePROTECT Desktop analyse les exécutions potentielles de fichiers et recherche les ransomware et autres programmes malveillants dans les couches de système d'exploitation et de mémoire afin d'empêcher la distribution de charges utiles malveillantes.
Protection des terminaux Mobiles	CylancePROTECT Mobile fournit une défense contre les menaces mobiles pour les terminaux iOS, Android et Chrome. Outre l'identification des programmes malveillants, CylancePROTECT Mobile non seulement détecte les applications chargées latéralement, les URL malveillantes dans les messages texte et d'autres risques de sécurité, mais recommande également des actions spécifiques pour éliminer la menace.
Détection et réponse aux attaques	CylanceOPTICS surveille vos terminaux Windows, macOS et Linux et vous informe lorsque votre entreprise est susceptible d'être victime d'une attaque. CylanceOPTICS recueille des informations à partir des terminaux et les agrège à l'aide de services cloud pour suivre, alerter et répondre aux évènements malveillants dès qu'ils se produisent. CylanceOPTICS peut arrêter les attaques avant qu'elles ne soient exécutées, et automatiser les enquêtes et la réponse aux attaques.

Fonctionnalité	Description
Sécurisation de l'accès à votre réseau et à vos services cloud	CylanceGATEWAY fournit un ZTNA (Zero Trust Network Access) aux utilisateurs des terminaux iOS, Android, Windows, et macOS pour sécuriser l'accès des utilisateurs au périmètre de votre réseau étendu et protéger votre réseau étendu contre les menaces. CylanceGATEWAY protège les terminaux en vous permettant de bloquer les connexions à des destinations Internet que vous ne souhaitez pas atteindre, même lorsque le terminal n'est pas connecté à votre réseau. CylanceGATEWAY protège votre réseau privé et vos services cloud en autorisant l'accès uniquement aux utilisateurs autorisés.
Protection des données sensibles	CylanceAVERT identifie et classe les données sensibles sur les terminaux Windows de l'environnement de votre entreprise afin de créer un inventaire de fichiers sensibles et avertit les utilisateurs spécifiés lorsque des données sensibles sont impliquées dans un évènement d'exfiltration. CylanceAVERT peut analyser les fichiers copiés sur un terminal USB, téléchargés vers un emplacement de navigateur ou un lecteur réseau, ou dans le corps du texte ou les pièces jointes des e-mails, et recommander une action corrective.
Travailler avec n'importe quelle plateforme UEM ou MDM	Cylance Endpoint Security peut être utilisé avec BlackBerry UEM pour fournir le plus haut niveau de sécurité et de gestion des points de terminaison afin de protéger votre entreprise contre un large éventail de menaces. Si vous disposez d'une plate-forme Unified Endpoint Management (UEM) ou Mobile Device Management (MDM) autre que BlackBerry UEM, vous pouvez utiliser Cylance Endpoint Security pour mieux protéger vos points de terminaison et les données qui transitent entre eux et votre réseau. Au fil du temps, des intégrations spécifiques avec des solutions MDM comme UEM et Microsoft Intune seront ajoutées à Cylance Endpoint Security pour améliorer votre capacité à gérer les terminaux en réponse aux menaces potentielles.

Architecture Cylance Endpoint Security



Composant	Description
BlackBerry Infrastructure	BlackBerry Infrastructure Est un réseau de données privées global réparti sur plusieurs régions, qui permet d'utiliser et de sécuriser des données en transit entre des milliers d'organisations et des millions d'utilisateurs à travers le monde. Il est conçu pour gérer efficacement le transport de données entre les services BlackBerry et les terminaux des utilisateurs finaux. Le système BlackBerry Infrastructure enregistre les informations de l'utilisateur pour l'activation de l'agent et de l'application CylancePROTECT Mobile, valide les informations de licence et maintient une connexion sécurisée avec les composants sur site installés derrière le pare-feu ainsi qu'avec les agents et l'application CylancePROTECT Mobile sur les terminaux des utilisateurs situés à l'intérieur et à l'extérieur du pare-feu.
CylancePROTECT	CylancePROTECT Desktop détecte et bloque les programmes malveillants sur les terminaux Windows, macOS et Linux à l'aide de techniques d'apprentissage automatique pour neutraliser les nouveaux programmes malveillants, virus, bots et variantes futures. CylancePROTECT Mobile détecte les programmes malveillants, les applications chargées latéralement, les URL malveillantes dans les messages texte et d'autres risques de sécurité sur les terminaux avec SE iOS, Android et Chrome, et recommande des mesures pour éliminer la menace.
CylanceOPTICS	CylanceOPTICS surveille les terminaux Windows, macOS et Linux et agrège les informations collectées pour détecter, suivre, alerter et répondre aux événements malveillants dès qu'ils se produisent. CylanceOPTICS peut vous aider à détecter les attaques dès le début et à automatiser les enquêtes et les réponses pour les arrêter avant qu'elles ne soient préjudiciable.
CylanceGATEWAY	CylanceGATEWAY protège l'accès au réseau privé et les applications cloud de votre entreprise, qui permettent aux utilisateurs de Windows, macOS, iOS et Android d'accéder à votre périmètre réseau étendu, et protège également votre réseau étendu contre les menaces.
CylanceAVERT	CylanceAVERT détecte et empêche la perte d'informations règlementaires et organisationnelles sensibles par le biais de sources externes. CylanceAVERT peut découvrir, classer et inventorier les informations sensibles de l'entreprise et fournir une détection des menaces pour empêcher les évènements d'exfiltration non autorisés.
Services cloud Cylance Endpoint Security	Les services Cloud Cylance Endpoint Security sont la matière grise de chaque fonctionnalité Cylance Endpoint Security. Les services Cloud pour différentes fonctionnalités utilisent l'IA, l'apprentissage automatique ou un moteur de risque basé sur la modélisation des utilisateurs pour traiter d'importants volumes de données complexes afin d'identifier les menaces et d'y répondre. Pour plus d'informations, reportez-vous à Comment Cylance Endpoint Security utilise la technologie avancée pour protéger les utilisateurs et les terminaux.
Console de gestion	La console de gestion cloud vous permet de configurer, de gérer et de surveiller toutes les fonctionnalités de Cylance Endpoint Security.

Composant	Description
Terminaux avec agents ou l'application CylancePROTECT Mobile	Les agents installés sur des terminaux Windows, macOS et Linux et l'application installée CylancePROTECT Mobile sur des terminaux avec un SE iOS, Android et Chrome communiquent avec Cylance Endpoint Security pour détecter les menaces potentielles et prendre des mesures pour protéger vos utilisateurs, vos terminaux et votre réseau.
BlackBerry Connectivity Node	Le BlackBerry Connectivity Node est un composant facultatif qui permet à Cylance Endpoint Security de synchroniser les utilisateurs et les groupes avec votre Microsoft Active Directory sur place ou votre annuaire LDAP. Cylance Endpoint Security peut synchroniser des utilisateurs et des groupes avec Entra Active Directory sans BlackBerry Connectivity Node.
CylanceGATEWAY Connector	CylanceGATEWAY Connector est un composant facultatif que vous pouvez installer derrière votre pare-feu et dans des réseaux de cloud privé pour établir un tunnel sécurisé entre BlackBerry Infrastructure et votre réseau privé. Le CylanceGATEWAY Connector permet aux utilisateurs de communiquer avec des serveurs de contenu et d'applications derrière votre pare-feu à l'aide de CylanceGATEWAY au lieu d'un VPN traditionnel.

Comment Cylance Endpoint Security utilise la technologie avancée pour protéger les utilisateurs et les terminaux

CylancePROTECT Desktop et CylancePROTECT Mobile s'appuient sur des services cloud de pointe pour déterminer si des logiciels, des fichiers et des sites Web sont potentiellement malveillants et constituent une menace pour la sécurité d'un terminal. Les services cloud CylancePROTECT utilisent l'IA sophistiquée, l'apprentissage automatique et des modèles mathématiques efficaces pour traiter de grands volumes de données provenant de sources mondiales, conserver et apprendre en continu des modèles et propriétés de ces données. Utilisez ces données pour faire des prévisions et des décisions intelligentes sur le potentiel de risque des logiciels, fichiers et destinations Internet en temps quasi réel. Les services CylancePROTECT évoluent en permanence pour faire face aux nouvelles cybermenaces, en fournissant une stratégie de sécurité agressive et proactive qui identifie les logiciels et sites Web malveillants avant qu'ils n'aient un impact sur l'infrastructure ou les utilisateurs des terminaux de votre entreprise.

Les services CylancePROTECT fournissent l'analyse des menaces pour les fichiers analysés par l'agent CylancePROTECT Desktop. Si un fichier est identifié comme malveillant, l'agent CylancePROTECT Desktop effectue toutes les actions d'atténuation que vous avez configurées (par exemple, alerte ou quarantaine). L'agent inclut un modèle de service local CylancePROTECT. Ainsi, si l'agent ne peut pas communiquer avec le cloud, il utilise le modèle local pour noter un fichier.

Les services CylancePROTECT sont un composant essentiel de plusieurs fonctionnalités CylancePROTECT Mobile, notamment la détection des programmes malveillants, l'analyse des messages SMS, et des contrôles réseau sécurisés. Si CylanceGATEWAY est activé, l'application CylancePROTECT Mobile utilise également l'apprentissage machine pour évaluer en continu le comportement de l'utilisateur et fournir des événements d'anomalie de réponse adaptative lorsque le modèle d'utilisation du réseau d'un utilisateur n'est pas cohérent avec le comportement passé. CylanceGATEWAY peut bloquer l'accès d'un utilisateur au réseau ou exiger une nouvelle authentification de l'utilisateur.

L'agent CylanceOPTICS sur les terminaux de bureau envoie les données qu'il collecte aux services cloud CylanceOPTICS. Les données sont agrégées et stockées dans la base de données cloud sécurisée CylanceOPTICS. Les services d'analyse des données CylanceOPTICS offrent des interprétations riches des

données du terminal auxquelles vous pouvez accéder dans la console de gestion. CylanceOPTICS utilise un moteur d'analyse de contexte (CAE) pour analyser et corréler les événements au fur et à mesure qu'ils se produisent sur les terminaux. Vous pouvez configurer CylanceOPTICS pour effectuer des actions de réponse automatisées lorsque le CAE identifie certains artefacts d'intérêt (par exemple, afficher une notification ou déconnecter l'utilisateur actuel), fournissant ainsi une couche supplémentaire de détection et de prévention des menaces pour compléter les fonctionnalités de CylancePROTECT Desktop.

Pour les terminaux de bureau avec l'agent CylanceGATEWAY, les services cloud utilisent l'apprentissage automatique pour créer un modèle comportemental basé sur l'activité de l'utilisateur et utiliser ce modèle pour connaître les écarts par rapport au comportement attendu de l'utilisateur. L'agent CylanceGATEWAY collecte des données sur le modèle d'utilisation du réseau d'un utilisateur et, de même, peut bloquer de manière dynamique l'accès au réseau de l'utilisateur et lui demander de s'authentifier avant de continuer.

L'agent CylanceAVERT identifie les fichiers sensibles sur un point de terminaison et avertit l'administrateur de toute tentative d'extraction de ces fichiers par e-mail, téléchargements de navigateur, lecteurs réseau ou terminaux USB. Si un fichier sensible est impliqué dans un évènement d'exfiltration, CylanceAVERT exécute l'action d'atténuation spécifiée par l'administrateur dans les paramètres de protection des informations. CylanceAVERT utilise la correspondance de mots-clés et la validation regex pour identifier les types de données sensibles qui déclenchent un évènement d'exfiltration.

Qu'est-ce que CylancePROTECT Desktop ?

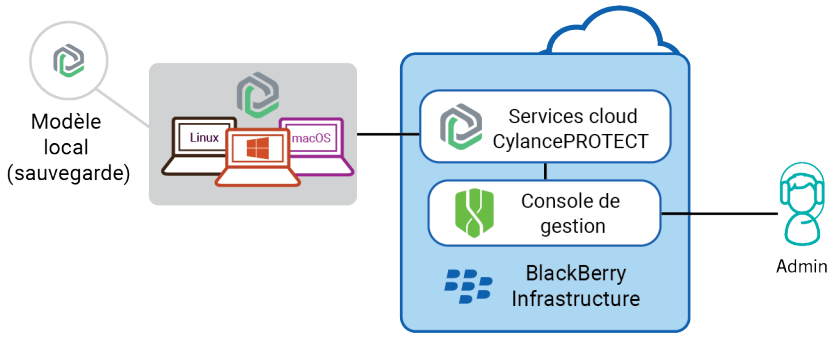
CylancePROTECT Desktop détecte et bloque les programmes malveillants avant qu'ils n'affectent un terminal. BlackBerry utilise une approche mathématique de l'identification des programmes malveillants, à l'aide de techniques d'apprentissage automatique au lieu de signatures réactives, de systèmes basés sur la confiance ou de bacs à sable. Cette approche neutralise les nouveaux programmes malveillants, virus, bots et variantes futures. CylancePROTECT Desktop analyse les exécutions potentielles de fichiers à la recherche de programmes malveillants dans les couches de système d'exploitation et de mémoire afin d'empêcher la distribution de charges utiles malveillantes.

L'agent CylancePROTECT Desktop est conçu pour utiliser un minimum de ressources système. L'agent traite les fichiers ou les processus qui s'exécutent en priorité car ces événements peuvent être malveillants. Les fichiers qui se trouvent simplement sur disque (dans le stockage mais qui ne sont pas en cours d'exécution) ont une priorité plus faible, car bien qu'ils puissent être malveillants, ils ne constituent pas une menace immédiate.

Principales fonctionnalités de CylancePROTECT Desktop

Fonctionnalité	Description
Détecter et mettre en quarantaine les fichiers malveillants	CylancePROTECT Desktop fournit des options de gestion des fichiers qu'il détecte comme dangereux ou anormaux. Vous pouvez ajouter des fichiers identifiés dans des événements de menace à une liste de quarantaine ou à une liste sécurisée pour gérer les événements futurs.
Se protéger contre les exploits de mémoire	CylancePROTECT Desktop fournit des options pour gérer les exploits de mémoire, y compris les injections de processus et les escalades. Vous pouvez également ajouter des fichiers exécutables à une liste d'exclusion pour autoriser leur exécution lorsqu'une stratégie de terminal est appliquée.
Bloquer les scripts malveillants	CylancePROTECT Desktop surveille et protège contre les scripts malveillants qui s'exécutent dans votre environnement. L'agent CylancePROTECT Desktop peut détecter le script et son chemin avant son exécution et le bloquer.
Bloquer les menaces provenant des terminaux de stockage USB	CylancePROTECT Desktop contrôle la façon dont les terminaux de stockage USB peuvent se connecter aux terminaux de votre organisation. Vous pouvez autoriser ou bloquer les terminaux de stockage USB, y compris les clés USB, les disques durs externes et les smartphones.
Recevoir des alertes immédiates	BlackBerry Protect Desktop surveille l'exécution de processus malveillants et vous alerte en cas de tentative d'exécution anormale ou dangereuse.
Détecter les terminaux inactifs	Si l'agent CylancePROTECT Desktop est resté hors contact pendant un certain temps, l'état du terminal devient inactif. Vous pouvez consulter les terminaux inactifs pour déterminer s'ils doivent être supprimés de la console de gestion.
Protéger les machines virtuelles	CylancePROTECT Desktop ne consomme pas autant de ressources par invité, car la technologie ne nécessite pas d'analyses quotidiennes des disques. CylancePROTECT Desktop ne consomme pas autant de mémoire par client.

Architecture : CylancePROTECT Desktop



Élément	Description
Services cloud CylancePROTECT	CylancePROTECT Desktop détecte et bloque les programmes malveillants à l'aide de techniques d'apprentissage automatique pour neutraliser les nouveaux programmes malveillants, virus, bots et variantes futures. Les services cloud CylancePROTECT utilisent l'IA sophistiquée, l'apprentissage automatique et des modèles mathématiques efficaces pour traiter de grands volumes de données provenant de sources mondiales, conserver et apprendre en continu des modèles et propriétés de ces données. Utilisez ces données pour faire des prévisions et des décisions intelligentes sur le potentiel de risque des logiciels, fichiers et destinations Internet en temps quasi réel. Les services CylancePROTECT fournissent une notation relative aux menaces des fichiers analysés par l'agent CylancePROTECT Desktop. Le score détermine la mesure que l'agent doit prendre sur les fichiers, en fonction de la stratégie de terminal attribuée à l'agent.
Console de gestion	La console de gestion cloud vous permet d'afficher divers événements liés aux menaces, de gérer les stratégies de terminaux pour configurer les agents sur les points de terminaison et de gérer les listes globales pour les fichiers mis en quarantaine et sécurisés.
Terminaux avec l'agent CylancePROTECT Desktop	L'agent CylancePROTECT Desktop doit être installé sur un terminal (point de terminaison) pour le protéger. CylancePROTECT Desktop prend en charge les systèmes d'exploitation Windows, macOS et Linux.
Modèle local	L'agent CylancePROTECT Desktop de chaque point de terminaison conserve une copie secondaire du modèle que les services CylancePROTECT utilisent pour noter les fichiers. Si l'agent ne parvient pas à se connecter aux services CylancePROTECT, le modèle local calcule les notes des fichiers.

Qu‘est-ce que CylancePROTECT Mobile ?

CylancePROTECT Mobile est une solution de sécurité avancée qui identifie et prévient de manière proactive les cybermenaces sur les terminaux iOS, Android, et les systèmes d‘exploitation Chrome en temps réel, sans perturber la productivité de votre personnel.

CylancePROTECT Mobile utilise une combinaison de technologies de pointe, notamment :

- La console de gestion Web que vous utilisez pour gérer les terminaux mobiles, gérer les fonctionnalités de CylancePROTECT Mobile et afficher des détails sur les menaces mobiles
- L‘application CylancePROTECT Mobile qui analyse le terminal d‘un utilisateur à intervalles réguliers pour détecter les menaces et fournir une évaluation de sécurité globale. Dans la mesure du possible, l‘application donne à l‘utilisateur des instructions claires pour résoudre les menaces sans intervention de l‘administrateur
- Les services cloud CylancePROTECT qui utilisent l‘IA sophistiquée et l‘apprentissage automatique pour prendre en charge des fonctionnalités clés de CylancePROTECT Mobile, notamment l‘identification en temps réel des programmes malveillants et des URL dangereuses dans les messages texte

L‘intégration transparente de ces technologies crée un écosystème sécurisé où les données sont protégées et où les activités malveillantes sont identifiées sur les terminaux mobiles et éliminées de manière proactive. CylancePROTECT Mobile est facile à configurer, facile à comprendre et à utiliser pour les utilisateurs finaux et tire parti des technologies cloud qui s‘améliorent et deviennent toujours plus intelligentes.

Principales fonctionnalités de CylancePROTECT Mobile

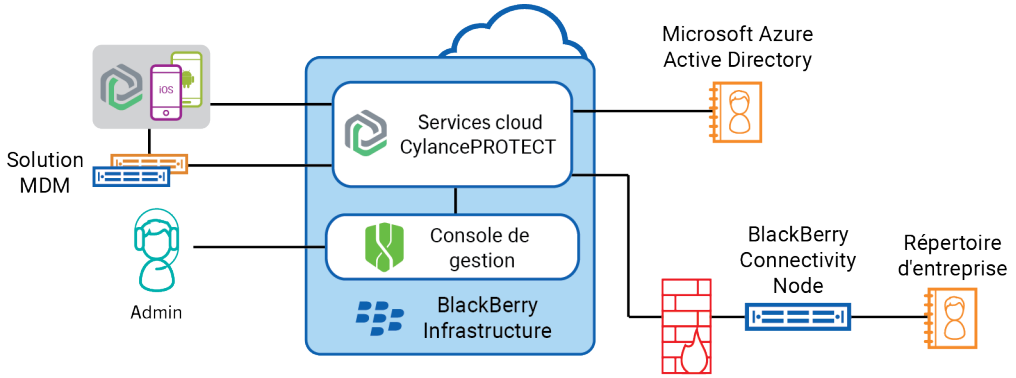
Fonctionnalité	Description
Détection des programmes malveillants pour les terminaux Android	L'application CylancePROTECT Mobile peut détecter les programmes malveillants sur un terminal Android et demander à l'utilisateur de désinstaller les applications malveillantes. L'application CylancePROTECT Mobile analyse les applications sur le terminal d'un utilisateur et télécharge les fichiers d'application sur les services cloud CylancePROTECT, qui utilisent l'IA et l'apprentissage automatique pour analyser le package d'application et produire un score de confiance qu'elle renvoie à l'application CylancePROTECT Mobile. Le score de confiance détermine si l'application analysée est sûre ou potentiellement malveillante. Lorsque les services CylancePROTECT déterminent qu'une application est potentiellement malveillante, l'application avertit l'utilisateur et fournit des informations supplémentaires. L'utilisateur peut appuyer sur une option de correction dans l'application pour accéder aux paramètres du terminal et désinstaller l'application malveillante. Une application est téléchargée sur les services CylancePROTECT si elle présente un hachage que les services n'ont pas encore traité. Si l'analyse de l'appareil trouve une application qui a déjà été examinée, elle utilise le score de confiance que les services CylancePROTECT ont déjà généré pour ce hachage d'application unique. Chaque fois qu'une application possède un nouveau hachage (par exemple, pour une nouvelle version), elle est téléchargée sur les services CylancePROTECT pour analyse et notation (si elle n'a pas déjà été téléchargée depuis un autre terminal).

Fonctionnalité	Description
Détection de chargement latéral pour les terminaux iOS et Android	Les applications chargées latéralement ne suivent pas les mêmes restrictions ou protections que les applications distribuées via les boutiques d'applications officielles. L'application CylancePROTECT Mobile peut détecter la présence d'une application sur le terminal d'un utilisateur, alerter l'utilisateur et le guider pour la désinstaller. Sur iOS, l'application CylancePROTECT Mobile peut détecter uniquement les certificats de développeur d'applications chargées latéralement auxquels l'utilisateur a choisi de faire confiance dans les paramètres du terminal. Un utilisateur ne peut pas utiliser une application chargée latéralement, sauf si le certificat du développeur de l'application a été approuvé. Sur Android, l'application CylancePROTECT Mobile identifie les applications chargées latéralement en fonction de la source d'installation. Les services cloud CylancePROTECT et l'application CylancePROTECT Mobile considèrent que les sources d'applications officielles, telles Google Play, le Amazon Appstore, et la boutique Samsung Galaxy, sont fiables. Les applications installées à partir de sources non fiables sont considérées comme chargées latéralement.
Analyse des URL dans les SMS sur les terminaux iOS	CylancePROTECT Mobile peut avertir les utilisateurs d'URL potentiellement malveillantes dans les SMS. Les nouveaux messages texte entrants provenant de contacts connus sont automatiquement considérés comme sûrs et seuls les messages provenant d'expéditeurs inconnus sont analysés et évalués. Lorsqu'un utilisateur reçoit un SMS contenant une URL, l'application CylancePROTECT Mobile envoie l'intégralité du message aux services cloud CylancePROTECT en temps réel. Les services CylancePROTECT utilisent des capacités d'apprentissage automatique avancées et des connaissances accumulées à partir de flux de renseignements sur les menaces pour fournir une évaluation instantanée de la sécurité du message. Lorsqu'une URL non sécurisée est détectée dans un message texte, le message est filtré vers le dossier des courriers indésirables. Pour protéger la confidentialité des utilisateurs, seuls les messages contenant des URL sont évalués. Aucune métadonnée ou identifiant utilisateur supplémentaire n'est collecté ou stocké.

Fonctionnalité	Description
Analyse des URL dans les SMS sur les terminaux Android	CylancePROTECT Mobile peut avertir les utilisateurs d'URL potentiellement malveillantes dans les SMS. Lorsqu'un utilisateur reçoit un SMS contenant une URL, l'URL non modifiée est envoyée aux services cloud CylancePROTECT n temps réel. L'analyse des SMS limitée à l'application SMS par défaut sur le terminal. Les nouveaux messages texte entrants provenant de contacts connus et d'expéditeurs inconnus sont analysés et évalués. Les services CylancePROTECT utilisent des capacités d'apprentissage automatique avancées et des connaissances accumulées à partir de flux de renseignements sur les menaces pour fournir une évaluation instantanée de la sécurité de l'URL. Si une URL est jugée dangereuse, l'application CylancePROTECT Mobile avertit l'utilisateur, fournit des détails et l'aide à supprimer le message texte. Pour protéger la confidentialité des utilisateurs, seuls les messages contenant des URL sont évalués. Aucune métadonnée ou identifiant utilisateur supplémentaire n'est collecté ou stocké.
Vérifications des réseaux et des Wi-Fi non sécurisés	CylancePROTECT Mobile vous protège contre les menaces réseau suivantes : • Connexions réseau dangereuses : sur les terminaux iOS et Android, CylancePROTECT Mobile l'application tente régulièrement de se connecter aux services cloud CylancePROTECT. Si la connexion échoue, CylancePROTECT Mobile détermine que le réseau n'est pas sécurisé. • Points d'accès Wi-Fi non sécurisés : sur les terminaux Android, l'application CylancePROTECT Mobile vérifie régulièrement les propriétés du point d'accès Wi-Fi actuel pour déterminer s'il est sécurisé. Vous pouvez configurer les algorithmes d'accès Wi-Fi que votre entreprise considère comme sécurisés et non sécurisés. Lorsque l'application CylancePROTECT Mobile détecte un réseau ou un point d'accès Wi-Fi non sécurisé, il est signalé dans l'application et dans la console de gestion.
Vérifications de sécurité du terminal	L'application CylancePROTECT Mobile vérifie les conditions spécifiques du terminal et les paramètres de sécurité et informe l'utilisateur des vulnérabilités potentielles aux cybermenaces. L'application vérifie les éléments suivants : • Si le mode développeur est activé (Android uniquement) • Si le chiffrement du disque est activé (Android uniquement) • Si le verrouillage de l'écran est activé (par exemple, un mot de passe ou une empreinte digitale) • indique si le terminal est débridé ou cracké • Indique si le terminal exécute une version du système d'exploitation que vous ne souhaitez pas prendre en charge • Indique si le modèle de terminal est un modèle que vous ne souhaitez pas prendre en charge Si l'application détecte une vulnérabilité, elle indique le niveau de risque potentiel et fournit des conseils à l'utilisateur pour résoudre le problème.

Fonctionnalité	Description
Vérifications d'attestation	Les services cloud CylancePROTECT peuvent effectuer régulièrement des vérifications d'attestation pour vérifier l'intégrité et la sécurité de l'application CylancePROTECT Mobile sur le terminal de chaque utilisateur. Sur les terminaux Android, les services cloud CylancePROTECT utilisent l'attestation Play Integrity, l'attestation SafetyNet et l'attestation de certificat matériel pour valider l'application CylancePROTECT Mobile. L'attestation Play Integrity remplace l'attestation SafetyNet. Les anciennes versions de l'application continueront à prendre en charge l'attestation SafetyNet jusqu'à ce que Google supprime cette prise en charge. Des contrôles d'attestation sont effectués quotidiennement. Vous pouvez également appliquer un niveau de correctif de sécurité minimal sur les terminaux. Si l'application détecte que le terminal ne répond pas au niveau de correctif requis, elle peut avertir l'utilisateur qu'il doit rechercher des mises à jour. Sur les terminaux iOS, les services cloud CylancePROTECT vérifient l'intégrité de l'application à l'aide de l'infrastructure DeviceCheck Apple. Les contrôles d'intégrité sont effectués quotidiennement. Sur les terminaux Samsung, les services cloud CylancePROTECT peuvent également utiliser l'attestation améliorée Samsung Knox à intervalles réguliers pour valider l'intégrité des terminaux. L'attestation améliorée Knox est basée sur le matériel et peut détecter la falsification des terminaux, le rootage, le déverrouillage OEM et la falsification de l'IMEI ou du numéro de série, en plus d'effectuer des contrôles d'intégrité des applications. En cas d'échec de l'attestation, les administrateurs peuvent afficher les détails dans la console de gestion.
Intégration avec les solutions MDM	Vous pouvez connecter Cylance Endpoint Security à Microsoft Intune pour permettre à Cylance Endpoint Security de signaler un niveau de risque de terminal à Intune. Le niveau de risque du terminal est calculé en fonction de la détection des menaces mobiles par l'application CylancePROTECT Mobile sur les terminaux gérés par Intune. Intune peut exécuter des actions d'atténuation en fonction du niveau de risque du terminal.
Fonctionnalités d'utilisation de l'application CylancePROTECT Mobile	Pour chaque fonctionnalité que vous choisissez d'activer dans l'application CylancePROTECT Mobile, vous pouvez choisir d'avertir les utilisateurs des menaces à l'aide des notifications du terminal, des e-mails ou de l'absence de notifications (les utilisateurs peuvent afficher les alertes de menace dans l'application CylancePROTECT Mobile). L'application CylancePROTECT Mobile pour Android 2.3.0.1640 et les versions ultérieures avertit l'utilisateur lorsqu'une nouvelle version de l'application est disponible dans Google Play. Au bout de 30 jours, l'application télécharge automatiquement la mise à jour et invite l'utilisateur à terminer la mise à jour et à redémarrer l'application. Après 60 jours, l'utilisateur ne peut pas utiliser l'application tant qu'il ne répond pas à l'invite de mise à niveau. L'application CylancePROTECT Mobile pour iOS prend en charge les mises à jour automatiques à partir de l'App Store.

Architecture : CylancePROTECT Mobile



Élément	Description
Services cloud CylancePROTECT	La console de gestion et l'application CylancePROTECT Mobile sur les terminaux des utilisateurs utilisent une connexion sécurisée pour communiquer avec les services cloud CylancePROTECT, qui sont responsables de la création et de la configuration des comptes d'utilisateur, de l'application des fonctionnalités et des paramètres CylancePROTECT Mobile aux terminaux et du traitement des événements et des alertes en temps réel. Les services CylancePROTECT utilisent l'IA et l'apprentissage automatique pour déterminer si les logiciels et les sites Web sont potentiellement malveillants et représentent une menace pour la sécurité d'un terminal. Ce moteur d'IA est un composant essentiel de plusieurs fonctionnalités CylancePROTECT Mobile, notamment la détection des programmes malveillants, l'analyse des SMS et la validation de la sécurité réseau. Au cœur de ce processus, le moteur d'IA active une stratégie de sécurité agressive et proactive, en identifiant les logiciels et sites Web malveillants avant qu'ils n'aient un impact sur l'infrastructure de votre organisation ou sur les utilisateurs de terminaux.
Console de gestion	La console de gestion cloud vous permet de gérer les terminaux mobiles, de configurer et de gérer les fonctionnalités CylancePROTECT Mobile et d'afficher l'état des terminaux ainsi que les alertes mobiles détectées par l'application CylancePROTECT Mobile.
BlackBerry Connectivity Node	BlackBerry Connectivity Node Est un composant facultatif qui permet Cylance Endpoint Security de synchroniser les utilisateurs et les groupes CylancePROTECT Mobile avec votre annuaire local Microsoft Active Directory ou LDAP. Cylance Endpoint Security peut synchroniser des utilisateurs et des groupes avec Entra Active Directory sans BlackBerry Connectivity Node.

Élément	Description
Terminaux avec l'application CylancePROTECT Mobile	L'application CylancePROTECT Mobile installée sur les terminaux de SE iOS, Android et Chrome analyse les terminaux à intervalles réguliers et vérifie leurs paramètres et les conditions pour identifier les menaces. Lorsque l'application détecte une menace, l'utilisateur peut afficher les détails dans l'application. Lorsque cela est possible, l'application fournit à l'utilisateur des instructions pour résoudre une menace et l'oriente vers les paramètres du terminal pour résoudre le problème.
Solution MDM	Vous pouvez également connecter Cylance Endpoint Security à Microsoft Intune pour permettre à Cylance Endpoint Security de signaler un niveau de risque de terminal à Microsoft Intune. Le niveau de risque du terminal est calculé en fonction de la détection des menaces mobiles par l'application CylancePROTECT Mobile sur les terminaux gérés par Intune. Intune peut exécuter des actions d'atténuation sur des terminaux en fonction du niveau de risque.

Qu'est-ce que CylanceOPTICS ?

CylanceOPTICS est une solution de détection et de réponse aux points de terminaison qui collecte et analyse les données des terminaux pour identifier et résoudre les menaces avant qu'elles n'affectent les utilisateurs et les données de votre organisation.

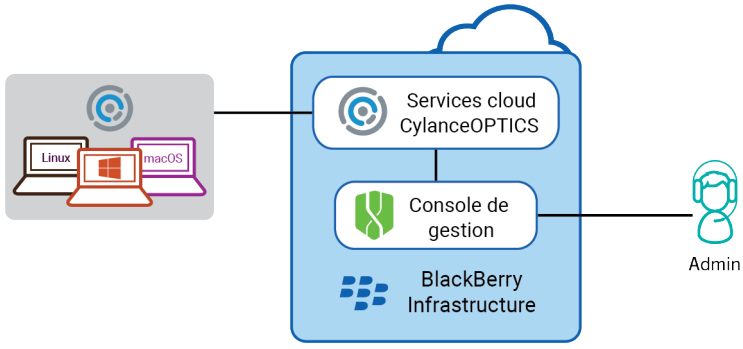
Vous activez un terminal Windows, macOS ou Linux pour CylanceOPTICS en installant l'agent CylanceOPTICS avec l'agent CylancePROTECT Desktop. L'agent CylanceOPTICS déploie des capteurs dans le système d'exploitation à différents niveaux et sous-systèmes pour surveiller et collecter un ensemble varié de données qui sont agrégées et stockées dans la base de données cloud CylanceOPTICS . Vous pouvez utiliser les données CylanceOPTICS pour détecter, analyser, diagnostiquer et configurer des réponses automatisées aux menaces basées sur les terminaux.

Principales fonctionnalités de CylanceOPTICS

Fonctionnalité	Description
Analyser les données CylanceOPTICS	Vous pouvez utiliser la console de gestion pour interroger les données du terminal collectées par l'agent CylanceOPTICS afin d'enquêter sur les incidents de sécurité et de découvrir les indicateurs de compromission. Lorsque CylanceOPTICS identifie un fichier comme une menace potentielle, vous pouvez le récupérer à partir du terminal pour une analyse plus approfondie. InstaQuery vous permet d'interroger un ensemble de terminaux sur un type spécifique d'artefact médico-légal et de déterminer si un artefact existe sur les terminaux et à quel point cet artefact est commun. La requête avancée est une évolution d'InstaQuery qui fournit des fonctionnalités de recherche plus granulaires à l'aide de la syntaxe EQL pour améliorer votre capacité à identifier les menaces.
Consulter les données CylanceOPTICS	Vous pouvez utiliser les fonctions de visualisation suivantes pour faciliter votre analyse approfondie : • La répartition des facettes InstaQuery fournit un affichage visuel interactif des différentes facettes impliquées dans une requête afin que vous puissiez identifier et suivre leurs chemins relationnels. • Focus Data vous permet de visualiser et d'analyser la chaîne d'événements, ainsi que les artefacts et facettes associés de ces événements, qui ont entraîné la création d'un logiciel malveillant ou d'une autre menace de sécurité sur un terminal.

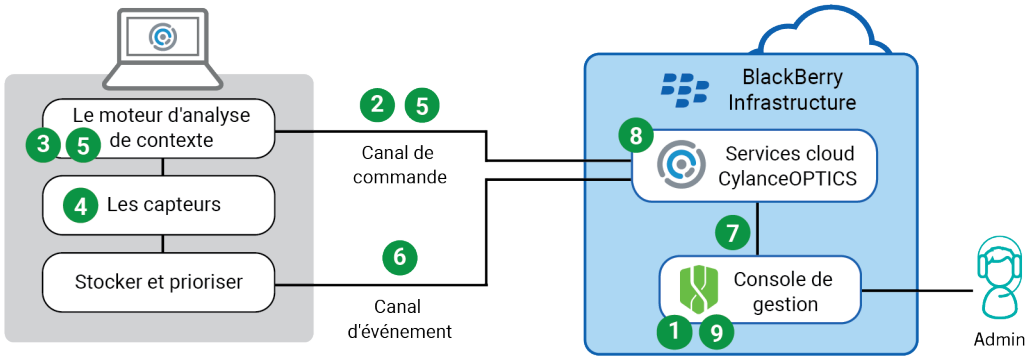
Fonctionnalité	Description
Détecter les événements et y répondre	CylanceOPTICS utilise le moteur d'analyse de contexte (CAE) pour analyser et corréler les événements qui se produisent sur les terminaux en temps quasi réel. Vous pouvez configurer CylanceOPTICS pour effectuer des actions de réponse automatisées lorsque le CAE identifie certains artefacts d'intérêt (par exemple, afficher une notification ou déconnecter l'utilisateur actuel), fournissant ainsi une couche supplémentaire de détection et de prévention des menaces pour compléter les fonctionnalités de CylancePROTECT Desktop. Vous pouvez personnaliser les capacités de détection d' CylanceOPTICS pour répondre aux besoins de votre entreprise. Vous pouvez créer des jeux de règles de détection avec la configuration de règles et de réponses de votre choix, cloner et modifier des règles de détection existantes ou créer vos propres règles personnalisées, et créer des exceptions de détection pour exclure des artefacts spécifiques de la détection.
Déployez des packages pour collecter des données	Vous pouvez utiliser la fonction de déploiement de package pour exécuter à distance et en toute sécurité un processus (par exemple un script Python) sur les terminaux CylanceOPTICS afin de collecter et de stocker les données souhaitées à un emplacement spécifié pour une analyse plus approfondie. Par exemple, vous pouvez exécuter un processus de collecte des données du navigateur. Vous pouvez utiliser les packages de collecte de données CylanceOPTICS disponibles dans la console de gestion ou créer les vôtres.
Verrouiller les terminaux pour isoler les menaces	Vous pouvez verrouiller un teminal infecté ou potentiellement infecté, en désactivant ses capacités réseau LAN et Wi-Fi pour arrêter l'activité de commande et de contrôle, l'exfiltration de données ou le mouvement latéral des logiciels malveillants. Diverses options de verrouillage sont disponibles pour répondre aux besoins de votre entreprise.
Envoyer des actions vers les terminaux	Vous pouvez utiliser la fonction de réponse à distance pour exécuter en toute sécurité des scripts et des commandes sur n'importe quel terminal CylanceOPTICS compatible directement à partir de la console de gestion, à l'aide d'une interface de ligne de commande familière.

Architecture : CylanceOPTICS



Composant	Description
Services cloud CylanceOPTICS	L'agent CylanceOPTICS envoie les données du terminal qu'il collecte aux services cloud CylanceOPTICS. Les données sont agrégées et stockées dans la base de données cloud sécurisée CylanceOPTICS. Les services d'analyse des données CylanceOPTICS offrent des interprétations riches des données de terminal auxquelles vous pouvez accéder via la console de gestion. Pour les terminaux dotés de la version d'agent CylanceOPTICS 2.x et antérieure, la base de données CylanceOPTICS est stockée localement sur le terminal. Les versions 3.0 et ultérieures agrègent, stockent, compressent et envoient automatiquement les données à la base de données cloud CylanceOPTICS à intervalles réguliers.
Console de gestion	La console de gestion basée sur le cloud vous permet de gérer les agents CylanceOPTICS installés sur les terminaux, d'interroger les données CylanceOPTICS pour enquêter sur les incidents de sécurité, de personnaliser les éléments surveillés par CylanceOPTICS et la façon dont il réagit aux évènements, et d'exécuter des actions en réponse aux menaces.
Terminaux avec l'agent CylanceOPTICS	Vous installez l'agent CylanceOPTICS sur les terminaux Windows, macOS et Linux. L'agent déploie des capteurs sur le système d'exploitation du terminal pour surveiller et collecter les données utilisées pour identifier les menaces et déclencher des réponses automatisées.

Flux de données : détection et réponse aux événements et stockage des données d'événement (CylanceOPTICS 3.x et versions ultérieures)



1. Un administrateur utilise la console de gestion pour configurer les règles de détection et les attribue à une stratégie de terminal.
2. Les services cloud CylanceOPTICS envoient les règles de détection via une connexion WebSocket sécurisée à un terminal avec l'agent CylanceOPTICS. Les données de règle incluent également les réponses configurées pour chaque événement (par exemple, déconnecter tous les utilisateurs, suspendre les processus, etc.).
3. L'agent CylanceOPTICS prend en compte les règles de détection dans le moteur d'analyse de contexte (CAE) qu'il utilise pour analyser et mettre les événements en corrélation.
4. Les capteurs CylanceOPTICS détectent un événement.

5. Le CAE détermine si l'événement respecte une règle de détection. Si c'est le cas, effectuez l'une des opérations suivantes :
   - Si l'agent CylanceOPTICS est déjà configuré avec la réponse à l'événement, il exécute la réponse.
   - Si l'agent a besoin de données supplémentaires pour exécuter la réponse (par exemple, si la réponse nécessite un package de playbooks que le terminal ne possède pas encore), l'agent envoie les données de détection aux services cloud CylanceOPTICS via une connexion WebSocket sécurisée. Les services cloud CylanceOPTICS traitent la détection et fournissent les données dont l'agent a besoin pour exécuter la réponse.
6. L'agent hiérarchise et envoie les données d'événement aux services cloud CylanceOPTICS via un canal d'événement dédié à l'aide d'une connexion TLS sécurisée. Les services cloud CylanceOPTICS reçoivent et traitent les données d'événement, les stockant dans la base de données cloud CylanceOPTICS sécurisée.
7. Un administrateur utilise la console de gestion pour demander des données de détection ou pour lancer une requête InstaQuery, une requête avancée ou une requête Focus View. La console de gestion interagit avec les services cloud CylanceOPTICS via HTTP sur TLS.
8. Les services Cloud CylanceOPTICS valident et traitent la demande, récupèrent les données demandées à partir de la base de données cloud CylanceOPTICS et renvoient les données à la console de gestion.
9. Les données de détection, le résultat de la requête ou les données détaillées s'affichent dans la console de gestion.

Qu‘est-ce que CylanceGATEWAY ?

CylanceGATEWAY est une solution ZTNA (Zero Trust Network Access) basée sur l‘intelligence artificielle (IA) et basée sur le cloud qui permet à vos utilisateurs d‘accéder à votre périmètre réseau étendu et de protéger votre réseau étendu contre les menaces. Aujourd‘hui, les entreprises sont confrontées à un environnement difficile, les menaces de cybersécurité devenant de plus en plus sophistiquées et omniprésentes, tandis que le nombre de points de terminaison d‘entreprise connectés, et la quantité de données envoyées et stockées dans les services cloud, augmentent de manière exponentielle. CylanceGATEWAY assure la sécurité du réseau tout en renforçant et en améliorant l‘expérience réseau pour les utilisateurs finaux. CylanceGATEWAY ne fait aucune confiance à personne par défaut. Chaque utilisateur, point de terminaison et réseau est supposé être potentiellement hostile et aucun utilisateur ne peut accéder à quoi que ce soit tant qu‘il n‘a pas prouvé qui il est, que son accès est autorisé, qu‘il n‘agit pas de manière malveillante et que le réseau local auquel il est connecté n‘est pas compromis.

CylanceGATEWAY protège les terminaux iOS, Android, Windows 10, Windows 11 et macOS des utilisateurs en vous permettant de bloquer les connexions aux destinations Internet que vous ne souhaitez pas atteindre, même lorsque le terminal n‘est pas connecté à votre réseau. BlackBerry tient constamment à jour une liste toujours plus longue de destinations Internet dangereuses pour lesquelles il peut empêcher les points de terminaison de s‘y connecter. Si votre organisation souhaite également empêcher les utilisateurs de visiter des sites spécifiques qui ne répondent pas à vos normes d‘utilisation acceptables, vous pouvez créer des stratégies pour spécifier des destinations supplémentaires auxquelles tous les utilisateurs ou certains utilisateurs ou groupes ne peuvent pas accéder.

En plus de protéger les terminaux, CylanceGATEWAY protège l‘accès au réseau privé et aux applications reposant sur le cloud de votre entreprise en analysant en permanence si les actions des utilisateurs sont attendues ou anormales.

Principales fonctionnalités de CylanceGATEWAY

Fonctionnalité	Description
Mode de travail	Les utilisateurs peuvent activer et désactiver le mode de travail. Le mode de travail protège votre réseau et vos terminaux. Lorsqu';il est activé, chaque tentative d';accès au réseau est évaluée par rapport aux règles de la liste de contrôle d';accès (ACL) et aux paramètres de protection réseau spécifiés configurés pour votre environnement. La liste de contrôle d';accès définit les destinations autorisées et bloquées sur les réseaux privés et publics. En cas d';autorisation, le trafic réseau est envoyé aux services cloud CylanceGATEWAY via un tunnel sécurisé.

Fonctionnalité	Description
Prise en charge du mode sans échec pour macOS et Windows	Vous pouvez activer le mode sans échec pour les utilisateurs. Grâce au mode sans échec, CylanceGATEWAY empêche les applications et les utilisateurs d';accéder à des destinations potentiellement malveillantes et met en application une stratégie d';utilisation acceptable (SUA) en interceptant les demandes DNS. Les services cloud CylanceGATEWAY évaluent chaque requête DNS par rapport aux règles ACL configurées et aux paramètres de protection réseau (par exemple, Tunnellisation DNS et détections Du jour zéro telles que Algorithme de génération de domaine (DGA), Hameçonnage et Programmes malveillants), puis demandent à l';agent d';autoriser ou de bloquer la demande en temps réel. En cas d';autorisation, la demande DNS est exécutée normalement sur le réseau porteur. Dans le cas contraire, l';agent CylanceGATEWAY remplace la réponse normale et empêche l';accès. **Remarque :** Lorsqu';il est activé, le mode sans échec protège l';ensemble du DNS qui n';utilise pas le tunnel CylanceGATEWAY (par exemple, accès au tunnel par application ou tunnellisation fractionnée).
Démarrez l';agent ou activez automatiquement le mode de travail sur macOS et Windows	Dans la stratégie de service Gateway, vous pouvez forcer l';agent CylanceGATEWAY sur les terminaux macOS ou Windows à s';exécuter automatiquement lorsque les utilisateurs se connectent, ou à activer automatiquement le mode de travail au démarrage de l';agent. Vos paramètres de stratégie peuvent remplacer les paramètres Démarrer CylanceGATEWAY lorsque je me connecte et Activer le mode de travail automatiquement de l';agent, mais les utilisateurs peuvent toujours activer et désactiver manuellement le mode de travail après le démarrage ou la fermeture de l';agent.
Intégrer des solutions MDM	Vous pouvez connecter Cylance Endpoint Security à BlackBerry UEM ou à Microsoft Intune afin que Cylance Endpoint Security puisse vérifier si les terminaux iOS ou Android sont gérés par UEM ou Intune. Vous pouvez spécifier si les terminaux doivent être gérés par UEM ou Intune avant de pouvoir utiliser CylanceGATEWAY. Pour en savoir plus sur les services réseau, consultez la section Connexion de Cylance Endpoint Security aux solutions MDM pour vérifier si les terminaux sont gérés.
Accès au tunnel par application sur macOS et iOS	Sur les terminaux macOS et iOS, sous Gestion des terminaux mobiles (MDM), vous pouvez désigner les applications autorisées à utiliser le tunnel Mode de travail CylanceGATEWAY. Vous pouvez ainsi autoriser l';utilisation professionnelle de terminaux personnels sans étendre l';accès au mode de travail à toutes les applications d';un terminal.
Prise en charge du tunnel par application sur Windows et Android	Sur les terminaux Windows et Android, vous pouvez spécifier ou restreindre les applications pouvant utiliser le tunnel CylanceGATEWAY.
Évaluation continue des destinations réseau	BlackBerry utilise l';apprentissage automatique, la réputation d';IP et l';évaluation des risques pour maintenir une liste en constante évolution des destinations Internet malveillantes. CylanceGATEWAY empêche les terminaux de se connecter à des domaines d';hameçonnage connus et inconnus et aux destinations IP et FQDN associées, ce qui évite à votre entreprise de compiler et de gérer manuellement sa propre liste.

Fonctionnalité	Description
Protection contre les menaces	CylanceGATEWAY utilise l'apprentissage automatique pour protéger en permanence le réseau de votre entreprise contre les menaces en surveillant en permanence les connexions réseau pour détecter les menaces potentielles. Lorsqu'une anomalie est identifiée, elle est ensuite bloquée ou signalée en fonction du niveau de risque défini dans les paramètres de protection réseau. • Les points d'accès sont protégés contre les menaces réseau émergentes et les destinations malveillantes établies. Anomalies identifiées (par exemple, jour zéro, domaines d'hameçonnage et balises de commande et de contrôle (C2)) • Les anomalies de tunnellisation DNS sont détectées sur la base de l'analyse de CylanceGateway sur le trafic DNS du client vers le serveur DNS du hackeur.
Évaluer le niveau de risque d'une destination réseau	Vous pouvez utiliser la console de gestion pour évaluer le niveau de risque et identifier la catégorie et la sous-catégorie des destinations réseau telles qu'elles seraient analysées et déterminées par les services cloud CylanceGATEWAY.
Prise en charge de plusieurs réseaux privés	Vous pouvez déployer plusieurs CylanceGATEWAY Connectors à partir d'un même locataire Cylance Endpoint Security pour autoriser l'accès à plusieurs de vos réseaux privés (par exemple, des segments, des centres de données et des VPC) qui se trouvent dans un environnement sur site et dans le cloud. Vous pouvez afficher les CylanceGATEWAY Connectors qui sont associés à chaque groupe de connecteurs spécifié.
Accès réseau privé segmenté	Vous pouvez installer CylanceGATEWAY Connectors sur site et sur des réseaux cloud privés pour fournir un accès réseau aux terminaux distants sans modifier la topologie ou le routage du réseau, et sans ouvrir de pare-feu pour le trafic entrant. L'accès via CylanceGATEWAY offre une isolation solide ; seules les parties du réseau que vous choisissez sont exposées aux points de terminaison, et les points de terminaison ne sont pas exposés à l'ensemble du réseau privé. Le CylanceGATEWAY Connector peut être déployé dans un environnement AWS vSphere ESXi Microsoft Entra ID ou Hyper-V.
Surveillance de l'accès réseau et des modèles de trafic	Le tableau de bord CylanceGATEWAY dans la console de gestion affiche plusieurs widgets montrant les connexions, les modèles d'utilisation et les alertes pour vous aider à surveiller le trafic réseau.
Spécifier les configurations de protection réseau	Dans l'écran Protection réseau, vous pouvez spécifier si les évènements réseau autorisés (par exemple, les réputations de destination et les détections de signature) inférieurs au niveau de risque minimum défini sont affichés sous forme d'anomalies dans l'écran Évènements réseau. Si les évènements autorisés sont désactivés, ils s'affichent en tant que trafic autorisé normal. En outre, vous pouvez configurer la prise en charge de la solution SIEM ou du serveur syslog pour envoyer uniquement des évènements bloqués. Ces fonctionnalités offrent un contrôle plus granulaire de la protection réseau et de la solution SIEM ou du serveur syslog, et peuvent contribuer à réduire le volume d'alertes.
Spécifier les paramètres de protection réseau à envoyer vers la vue Alertes	Dans l'écran Protection réseau, vous pouvez spécifier les détections (par exemple, réputation de destination, détections de signature, tunnellisation DNS et jour zéro) que vous souhaitez envoyer vers la vue Alertes. Les évènements ACL bloqués et autorisés ne sont pas partagés dans la vue Alertes. Cette fonction permet un contrôle plus granulaire des alertes affichées dans la vue Alertes.

Fonctionnalité	Description
Règles ACL propres au système d'exploitation	Vous pouvez créer des règles ACL et les appliquer à un système d'exploitation spécifique. Par exemple, vous pouvez autoriser l'accès à certaines ressources uniquement aux terminaux de bureau (macOS et Windows).
Configuration SaaS en un clic	Vous pouvez facilement configurer l'accès aux applications SaaS à l'aide des services réseau. CylanceGATEWAY rationalise la prise en charge des applications SaaS et réduit le temps nécessaire pour activer la connectivité des applications SaaS dans les règles ACL que vous configurez pour votre environnement. Pour plus d'informations sur les services réseau, consultez la section Définir des services réseau.
Filtrage du contenu	Les règles ACL et les paramètres de protection réseau que vous configurez pour votre environnement filtrent le contenu et les destinations auxquels vos utilisateurs peuvent accéder. Cette solution utilise l'apprentissage machine et les règles ACL pour s'assurer que les utilisateurs et les terminaux respectent les exigences règlementaires et d'utilisation acceptable de votre entreprise.
Rapports sur les détails de la NAT	Vous pouvez filtrer les évènements en fonction de l'adresse IP du tunnel (adresse IP source BlackBerry) pour identifier l'adresse IP du tunnel dont se servent les utilisateurs pour accéder à des destinations externes. Le système CylanceGATEWAY Connector fournit des informations supplémentaires sur les flux UDP et TCP qui accèdent à votre réseau privé via le tunnel après l'application de la traduction d'adresses réseau (NAT) (par exemple, Adresse IP source de la NAT privée et Port source privé). Cela vous permet d'identifier l'adresse IP source et le numéro de port d'un évènement qui a été identifié comme potentiellement malveillant ou bloqué et qui passe par votre réseau privé.
Pare-feu d'accès Web	CylanceGATEWAY protège les terminaux et vos réseaux privés en filtrant, surveillant et bloquant le trafic vers des destinations suspectes. CylanceGATEWAY complète cela en appliquant les règles ACL qui sont configurées pour votre environnement et les séries de protection du réseau que vous avez spécifiées. Pour plus d'informations : • Surveillance des connexions réseau dans le contenu Administration. • Contrôle de l'accès réseau à l'aide des règles ACL dans le contenu relatif à la configuration.

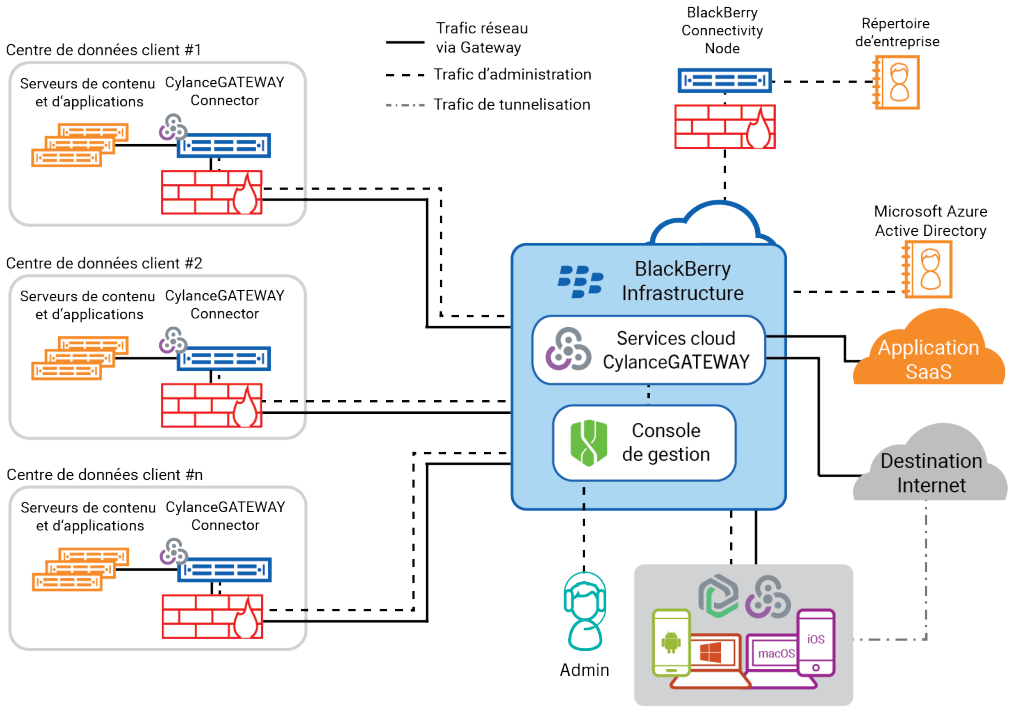
Fonctionnalité	Description
Prise en charge des services épinglés par IP	La plupart des applications SaaS permettent l'épinglage IP source pour limiter l'accès aux connexions à partir d'une plage spécifique d'adresses IP approuvées. En limitant les utilisateurs aux connexions uniquement via les points d'entrée approuvés, les entreprises disposent d'un niveau supplémentaire de vérification garantissant que l'utilisateur est autorisé à utiliser le service. Votre entreprise utilise peut-être déjà cette méthode pour limiter l'accès à une application SaaS aux connexions à partir des adresses IP utilisées par les terminaux connectés au réseau de votre entreprise. Pour les utilisateurs travaillant à distance sans utiliser CylanceGATEWAY, cela signifie que tout le trafic entre les terminaux distants et une application SaaS doit transiter par VPN vers votre réseau, puis vers l'application SaaS. CylanceGATEWAY vous permet de réserver des adresses IP CylanceGATEWAY dédiées à votre organisation. Vous pouvez utiliser ces adresses IP pour l'épinglage IP source en plus des adresses IP de votre entreprise, ce qui offre le même niveau de sécurité sans que les utilisateurs distants soient connectés au VPN de votre entreprise.
Technologie de tunnel de pointe	CylanceGATEWAY fournit un chiffrement avancé de couche 3 pour les tunnels IP transportant du trafic TCP, UDP, ICMP et en temps réel, à faible latence.
Prise en charge Android et iOS	L'application CylancePROTECT Mobile envoie le trafic aux services cloud CylanceGATEWAY via le tunnel, et fournit aux utilisateurs des statistiques de connexion, des informations d'état, et la possibilité de désactiver le mode de travail et de cesser d'utiliser CylanceGATEWAY pour les connexions.
Prise en charge Windows 10, Windows 11 et macOS	L'agent CylanceGATEWAY que vous installez sur les terminaux envoie le trafic aux services cloud CylanceGATEWAY via le tunnel, et fournit aux utilisateurs des statistiques de connexion, des informations d'état, et la possibilité de désactiver le mode de travail et de cesser d'utiliser CylanceGATEWAY pour les connexions.
Tunnellisation fractionnée	Vous pouvez autoriser les utilisateurs distants à se connecter à des sites Internet publics sécurisés directement sur Internet sans avoir à effectuer de tunnellisation via CylanceGATEWAY. Lorsque cette option est activée, les requêtes DNS fractionnées permettent d'effectuer des recherches DNS pour les domaines répertoriés dans la configuration Réseau privé > DNS > Zone de recherche directe via le tunnel où les contrôles d'accès au réseau sont appliqués. Toutes les autres recherches DNS sont effectuées à l'aide de votre DNS local. Si vous avez activé le mode sans échec, le trafic DNS qui n'utilise pas le tunnel Gateway est protégé par le mode sans échec. Les terminaux Android et Chromebook 64 bits utilisent le tunnel sur lequel des contrôles d'accès au réseau sont appliqués.

Architecture : CylanceGATEWAY

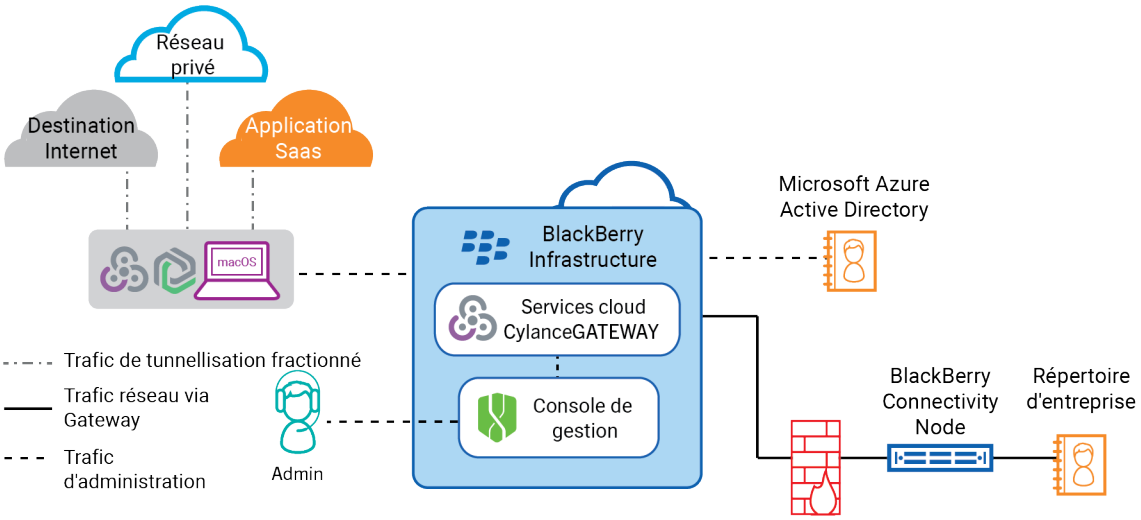
L'architecture CylanceGATEWAY a été conçue pour vous aider à protéger les terminaux des utilisateurs et votre réseau étendu contre les menaces. Les schémas suivants illustrent l'architecture de CylanceGATEWAY dans les deux modes de fonctionnement.

- Mode de travail : le mode de travail établit un tunnel sécurisé entre les terminaux et les ressources réseau via les services cloud CylanceGATEWAY, et protège l'ensemble du trafic sur ce chemin.
- Mode sans échec : le mode sans échec étend les règles ACL du locataire et la protection du point de terminaison pour les terminaux macOS Windows. S'il est activé, le mode sans échec prend automatiquement effet lorsque le mode de travail est désactivé, garantissant ainsi la protection continue des terminaux.

CylanceGATEWAY : mode de travail activé



CylanceGATEWAY : mode sans échec activé



Composant	Description
Services cloud CylanceGATEWAY	CylanceGATEWAY est un service cloud qui propose un accès réseau Zero Trust pour fournir à vos utilisateurs un accès à votre périmètre réseau étendu, et protéger les terminaux et votre réseau étendu contre les menaces. Les services cloud CylanceGATEWAY ont recours à l'apprentissage machine pour évaluer en permanence le comportement des utilisateurs et surveiller les connexions réseau. Les évènements d'anomalie réseau sont détectés lorsqu'un utilisateur CylanceGATEWAY tente de se connecter à une destination suspecte ou susceptible de contenir du contenu malveillant. Les anomalies détectées peuvent bloquer l'accès à une destination en fonction du seuil de risque configuré pour votre environnement. Certaines anomalies peuvent par ailleurs vous alerter d'une tentative de connexion, sans pour autant bloquer le trafic de l'utilisateur (par exemple, lorsque les volumes de chargement ou de téléchargement réseau d'un utilisateur ne sont pas cohérents avec le comportement antérieur).
Console de gestion	La console de gestion basée sur le cloud vous permet de configurer, de gérer et de surveiller CylanceGATEWAY, ainsi que les connexions établies par le biais de celui-ci.
CylanceGATEWAY Connector	Le CylanceGATEWAY Connector est un composant facultatif que vous pouvez installer derrière votre pare-feu et dans des réseaux privés afin d'établir un tunnel sécurisé entre les services CylanceGATEWAY et l'un de vos réseaux privés. Le CylanceGATEWAY Connector permet aux utilisateurs de communiquer avec des serveurs de contenu et d'applications derrière votre pare-feu à l'aide de CylanceGATEWAY au lieu d'un VPN traditionnel.
BlackBerry Connectivity Node	Le BlackBerry Connectivity Node est un composant facultatif qui permet à Cylance Endpoint Security de synchroniser les utilisateurs et les groupes avec votre Microsoft Active Directory sur site ou votre annuaire LDAP. Cylance Endpoint Security peut synchroniser des utilisateurs et des groupes avec Entra Active Directory sans BlackBerry Connectivity Node.
Terminaux mobiles avec l'application CylancePROTECT Mobile	CylanceGATEWAY prend en charge les terminaux iOS et Android. L'application CylancePROTECT Mobile installée sur les terminaux mobiles envoie le trafic Internet via un tunnel sécurisé vers les services cloud CylanceGATEWAY. Les utilisateurs peuvent activer et désactiver le mode de travail pour déterminer si le trafic de données utilise le tunnel vers les services cloud CylanceGATEWAY.

Composant	Description
Terminaux de bureau avec l'agent CylanceGATEWAY	CylanceGATEWAY prend en charge les terminaux macOS Windows 10 et 11. CylanceGATEWAY dispose de deux modes de fonctionnement : • Avec le mode de travail, l'agent CylanceGATEWAY envoie le trafic réseau aux services cloud CylanceGATEWAY via un tunnel sécurisé. Les utilisateurs peuvent activer et désactiver le mode de travail pour déterminer si le trafic de données utilise le tunnel. • Grâce au mode sans échec, CylanceGATEWAY empêche les applications et les utilisateurs d'accéder à des destinations potentiellement malveillantes et met en application une stratégie d'utilisation acceptable (SUA) en interceptant les demandes DNS. CylanceGATEWAY Cloud évalue chaque requête DNS par rapport aux règles ACL et aux paramètres de protection réseau configurés, puis demandent à l'agent d'autoriser ou de bloquer la demande en temps réel. En cas d'autorisation, la demande DNS est exécutée normalement sur le réseau porteur. Dans le cas contraire, l'agent CylanceGATEWAY remplace la réponse normale et empêche l'accès.
Applications SaaS	Les applications SaaS (Software-as-a-Service) fournissent des logiciels d'entreprise basés sur le cloud, mettant ainsi les applications et les données à la disposition des utilisateurs sur plusieurs terminaux. Les applications et les données résident principalement sur des serveurs cloud gérés par le fournisseur, ce qui facilite le déploiement et réduit les coûts d'infrastructure sur site, mais nécessite des mesures de sécurité qui s'étendent au-delà des pare-feu et autres méthodes de sécurité basées sur le périmètre. CylanceGATEWAY peut aider à sécuriser l'accès des utilisateurs aux applications SaaS sans exiger que le trafic passe par le réseau privé de votre entreprise en activant l'épinglage d'adresses IP sources.
Destinations Internet	Les destinations Internet publiques incluent tout site Web, toute application SaaS ou toute autre entité avec une adresse IP à laquelle une application client peut se connecter sur Internet. BlackBerry tient à jour une liste toujours plus longue de destinations connues pour être malveillantes. CylanceGATEWAY peut empêcher les applications sur les terminaux de se connecter aux destinations de la liste. Si vous activez la tunnellisation fractionnée, le trafic entre les terminaux et les sites publics sécurisés que vous spécifiez peut passer directement sur Internet au lieu de passer par CylanceGATEWAY.

Comment CylanceGATEWAY envoie les données à l'aide du mode de travail

Lorsque vos utilisateurs tentent d'accéder à des destinations sur le réseau privé ou sur une destination Internet publique, ils ne peuvent y accéder que s'ils sont explicitement autorisés par les règles de la liste de contrôle d'accès (ACL). Chaque tentative d'accès au réseau est évaluée par rapport aux règles ACL et aux paramètres de protection réseau spécifiés configurés pour votre environnement. Si une règle ACL bloque une destination, CylanceGATEWAY bloque la connexion et n'achemine pas le trafic. Si une règle ACL permet aux utilisateurs d'accéder au réseau privé ou à une destination Internet publique, la connexion est réévaluée toutes les cinq minutes et les règles ACL sont réappliquées. Si le niveau de risque d'un utilisateur a changé ou si la réputation de

la destination a été mise à jour depuis l'établissement de la tentative d'accès, la connexion peut être déconnectée. Lorsqu'une règle ACL permet aux utilisateurs d'accéder à une destination, la connexion peut ensuite être bloquée ou alertée en fonction des anomalies identifiées et du niveau de risque défini pour les paramètres de protection réseau.

- Si le volume de chargement ou de téléchargement d'un utilisateur a changé, CylanceGATEWAY signale tout trafic inhabituel, mais ne bloque pas le trafic de l'utilisateur.
- Si l'utilisateur tente d'accéder à une destination figurant sur la liste des destinations Internet dangereuses de BlackBerry ou qui vient d'être identifiée comme malveillante, et que le seuil de risque de protection réseau est élevé, l'accès de l'utilisateur est bloqué.

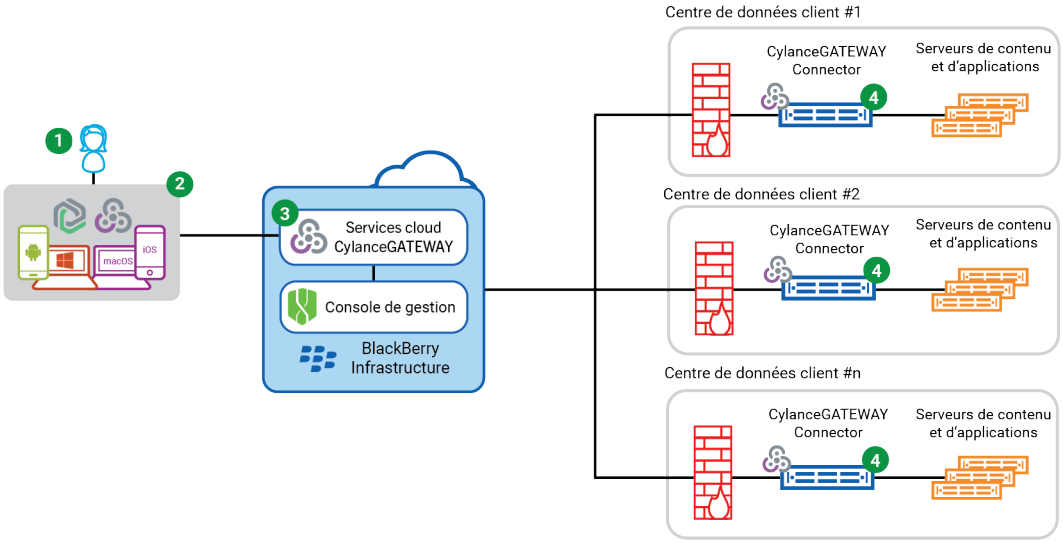
Lorsque CylanceGATEWAY est actif sur un terminal, CylanceGATEWAY achemine le trafic réseau de la manière suivante.

Destination	Action
Destination autorisée sur le réseau privé	Les utilisateurs peuvent accéder aux destinations de votre réseau privé uniquement s'ils sont explicitement autorisés par les règles de la liste de contrôle d'accès (ACL). Les règles ACL évaluent chaque tentative d'accès au réseau et si une règle correspond, elles permettent d'accéder au réseau privé. Toutes les données entre l'unité et votre réseau privé sont chiffrées à l'aide d'une technologie de tunnel de pointe et acheminées via des tunnels sécurisés depuis l'application CylancePROTECT Mobile ou l'agent CylanceGATEWAY vers le BlackBerry Infrastructure, puis depuis le BlackBerry Infrastructure vers le CylanceGATEWAY Connector installé derrière votre pare-feu.
Destination Internet autorisée	Les utilisateurs peuvent se connecter à n'importe quelle destination Internet publique uniquement s'ils sont explicitement autorisés par vos règles ACL. Les règles ACL évaluent chaque tentative d'accès au réseau et si une règle correspond, elles permettent d'accéder à la destination. Les connexions à des destinations Internet publiques sont acheminées via le tunnel sécurisé entre l'application CylancePROTECT Mobile ou l'agent CylanceGATEWAY et le BlackBerry Infrastructure puis CylanceGATEWAY achemine le trafic vers la destination. Si vous activez la tunnellisation fractionnée, le trafic vers des destinations Internet sécurisées est acheminé directement vers la destination plutôt que via le tunnel vers CylanceGATEWAY. Par exemple, vous pouvez choisir de réduire le trafic envoyé par CylanceGATEWAY en autorisant le trafic vers des sites publics sûrs d'être acheminé directement vers la destination.
Application SaaS autorisée	Par défaut, les connexions aux applications SaaS sont acheminées de la même manière que les connexions à d'autres destinations Internet. Si vous activez l'épinglage d'adresses IP source, vous pouvez configurer votre locataire d'application SaaS pour qu'il n'accepte que les connexions des adresses IP de votre organisation et CylanceGATEWAY.
Destination bloquée sur le réseau privé	Les utilisateurs peuvent accéder aux destinations de votre réseau privé uniquement s'ils sont explicitement autorisés par les règles ACL. Si la destination n'est pas autorisée, CylanceGATEWAY bloque la connexion et n'achemine pas le trafic vers CylanceGATEWAY Connector. Lorsque les utilisateurs tentent d'accéder à une destination et qu'elle est bloquée par une règle ACL, la tentative et le motif s'affichent sur l'écran Avertissement de l'agent CylanceeGATEWAY de l'utilisateur.

Destination	Action
Destination Internet bloquée	Si une destination est explicitement bloquée par vos règles ACL ou définie comme potentiellement dangereuse par BlackBerry, CylanceGATEWAY bloquera la connexion. Lorsque les utilisateurs tentent d'accéder à une destination et qu'elle est bloquée par une règle ACL, la tentative et le motif s'affichent sur l'écran Avertissement de l'agent de l'utilisateur CylanceGATEWAY.

Flux de données : accès à un serveur d'applications ou de contenu sur votre réseau privé

Ce flux de données décrit la façon dont les données transitent entre les terminaux et les serveurs de vos réseaux privés à l'aide de CylanceGATEWAY.

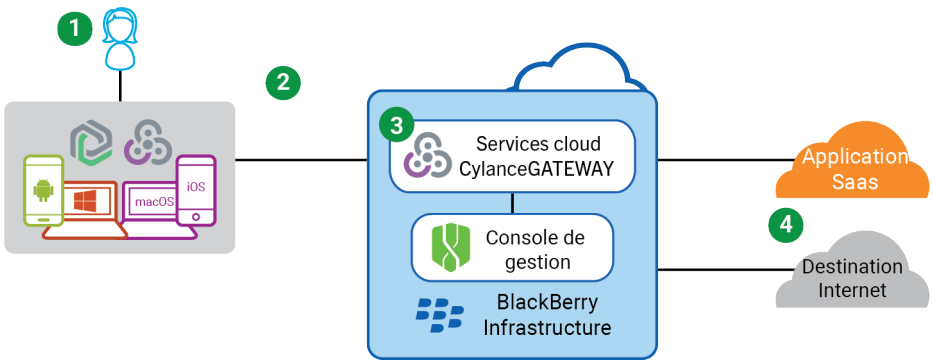


Le schéma ci-dessus illustre la séquence suivante.

1. L'utilisateur active le mode de travail, ouvre une application et tente d'accéder à une ressource sur l'un de vos réseaux privés.
2. L'application CylancePROTECT Mobile pour Android ou iOS ou l'agent CylanceGATEWAY pour Windows ou macOS sur le terminal qui achemine la connexion via un tunnel sécurisé vers CylanceGATEWAY dans BlackBerry Infrastructure.
3. CylanceGATEWAY effectue les actions suivantes :
   a. Détermine, sur la base des règles de la liste de contrôle d'accès (ACL), si l'utilisateur a accès à cet emplacement sur le réseau privé.
   b. Si l'utilisateur dispose d'un accès, achemine la connexion via un tunnel sécurisé vers CylanceGATEWAY Connector.
4. CylanceGATEWAY Connector achemine la connexion vers sa destination sur le réseau privé.

Flux de données : accès à une application cloud ou destinations Internet

Ce flux de données décrit comment les données voyagent entre les terminaux et une application SaaS basée sur le cloud ou une destination Internet publique en utilisant CylanceGATEWAY.



Le schéma ci-dessus illustre la séquence suivante.

1. L'utilisateur active le Mode travail, ouvre une application et tente d'accéder à une application ou une destination basée sur le cloud sur l'Internet public.
2. L'application CylancePROTECT Mobile pour Android ou iOS ou l'agent CylanceGATEWAY pour Windows ou macOS sur le terminal envoie les données chiffrées à travers un tunnel sécurisé pour CylanceGATEWAY dans le BlackBerry Infrastructure.
3. CylanceGATEWAY effectue les actions suivantes :
   a. Détermine, sur la base des règles de la liste de contrôle d'accès (ACL), si l'utilisateur a accès à cet emplacement.
   b. Si l'utilisateur a accès, envoie les données à l'application SaaS ou autorise l'accès à la destination Internet.
4. Si l'épinglage IP source est activé, l'application SaaS vérifie que la connexion provient d'une adresse IP associée à votre locataire CylanceGATEWAY avant d'autoriser l'accès.

Comment CylanceGATEWAY envoie des données à l'aide du mode sans échec

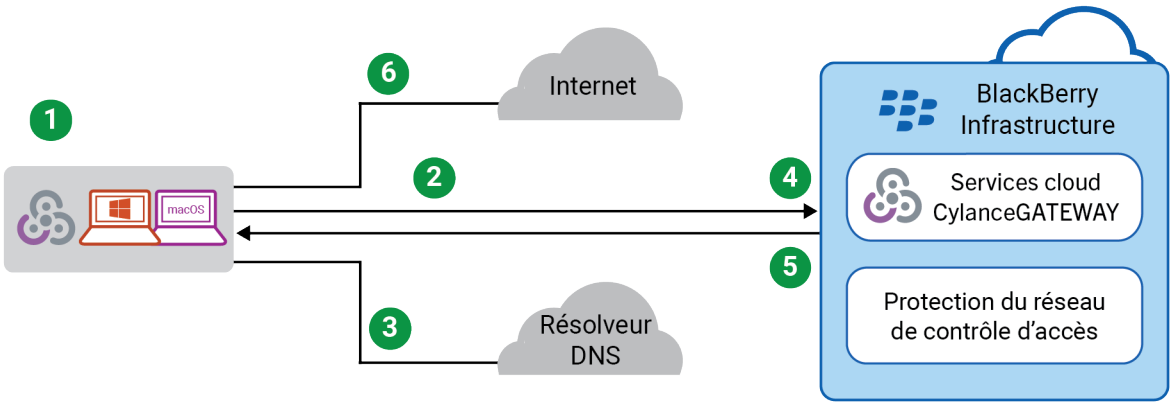
Lorsque vos utilisateurs tentent d'accéder à une destination Internet publique, ils y parviennent uniquement s'ils sont explicitement autorisés par les règles définies dans la liste de contrôle d'accès (ACL). Lorsque le mode sans échec est activé, CylanceGATEWAY empêche les utilisateurs d'accéder à des destinations potentiellement malveillantes et applique une politique d'utilisation acceptable (PUA) en interceptant les demandes DNS. Les services cloud CylanceGATEWAY évaluent chaque demande DNS par rapport aux règles ACL et aux paramètres de protection réseau configurés, puis demandent à l'agent d'autoriser ou de bloquer la demande en temps réel. Si la règle ACL bloque une destination, CylanceGATEWAY empêche l'accès. En cas d'autorisation, la demande DNS du réseau est autorisée à s'exécuter sur le réseau porteur.

Lorsque le mode sans échec est activé sur un terminal macOS ou Windows, CylanceGATEWAY envoie le trafic réseau de l'une des manières suivantes.

Destination	Action
Destination Internet autorisée	Les utilisateurs peuvent accéder à n'importe quelle destination Internet publique uniquement s'ils sont explicitement autorisés par vos règles ACL. Les règles ACL évaluent chaque tentative d'accès au réseau et si une règle correspond, elles permettent d'accéder à la destination. Si vous activez le mode sans échec, le trafic vers des destinations Internet sécurisées est acheminé vers la destination via le réseau porteur plutôt que via le tunnel CylanceGATEWAY. Si vous activez la tunnellisation fractionnée, le trafic vers des destinations Internet sécurisées est acheminé vers la destination via le réseau porteur et est protégé par le mode sans échec. Cela réduit le trafic envoyé par CylanceGATEWAY en autorisant l'acheminement du trafic vers des sites publics sûrs directement vers la destination.
Destination Internet bloquée	Si une destination est explicitement bloquée par vos règles ACL ou définie comme potentiellement dangereuse par BlackBerry, CylanceGATEWAY bloque la requête DNS. Lorsque les utilisateurs tentent d'accéder à une destination et qu'elle est bloquée par une règle ACL, la tentative et le motif s'affichent sur l'écran Avertissement de l'agent de l'utilisateur CylanceGATEWAY.

Flux de données : accès au contenu, aux applications et aux destinations Internet publiques à l'aide du mode sans échec

Ce flux de données décrit la façon dont les données transitent entre les terminaux et une destination Internet publique à l'aide du mode sans échec. Grâce au mode sans échec, CylanceGATEWAY empêche les applications et les utilisateurs d'accéder à des destinations potentiellement malveillantes et met en application une stratégie d'utilisation acceptable (SUA) en interceptant les demandes DNS. Les services cloud CylanceGATEWAY évaluent chaque demande DNS par rapport aux règles ACL et aux paramètres de protection réseau configurés, puis demandent à l'agent d'autoriser ou de bloquer la demande en temps réel. En cas d'autorisation, la demande DNS est exécutée normalement sur le réseau porteur. Dans le cas contraire, l'agent CylanceGATEWAY remplace la réponse normale et empêche l'accès.



Le schéma ci-dessus illustre la séquence suivante.

1. L'agent CylanceGATEWAY a activé le mode sans échec et l'utilisateur tente d'accéder à une destination Internet.

2. L'agent CylanceGATEWAY intercepte la demande DNS provenant du terminal et interroge les services cloud CylanceGATEWAY avec les informations de cette demande.
3. L'agent envoie la demande DNS au serveur DNS d'origine.
4. Les services cloud CylanceGATEWAY évaluent chaque requête par rapport aux règles ACL et aux paramètres de protection réseau configurés, puis demandent à l'agent d'autoriser ou de bloquer la demande.
5. Si l'accès est autorisé, l'agent délègue la réponse du serveur DNS d'origine en réponse à la demande DNS d'origine. Dans le cas contraire, l'agent injecte une réponse DNS qui bloque l'accès.
6. L'agent utilise les résultats d'une demande DNS autorisée pour accéder à une destination Internet.

Qu‘est-ce que CylanceAVERT ?

CylanceAVERT est une solution de protection des informations qui détecte et empêche la perte d‘informations règlementaires et organisationnelles sensibles par le biais de sources externes. CylanceAVERT peut découvrir, classer et inventorier les informations sensibles de l‘entreprise et fournir une détection des menaces pour empêcher les évènements d‘exfiltration non autorisés. En plus de fournir un inventaire de fichiers sensibles et une gestion des menaces, CylanceAVERT peut analyser les fichiers contenus dans le corps du texte ou les pièces jointes des e-mails, les copier sur un terminal USB, les copier sur un lecteur réseau ou les télécharger vers un emplacement de navigateur, et recommander une action corrective.

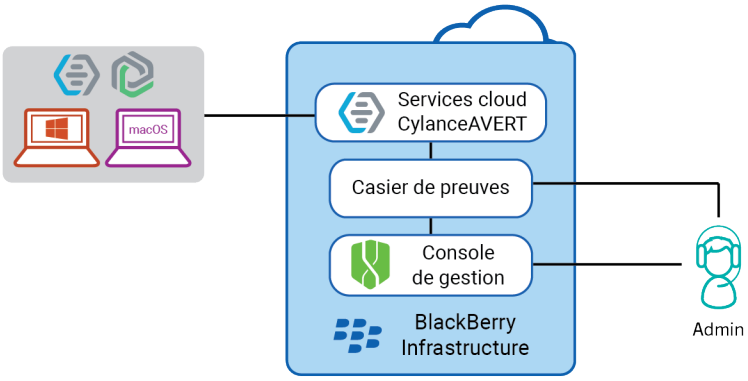
Lorsqu‘un utilisateur tente de télécharger des données sensibles à l‘aide d‘une clé USB, d‘un domaine de navigateur ou dans un e-mail, CylanceAVERT analyse le contenu et détermine s‘il est considéré comme sensible en fonction des stratégies de protection des informations. L‘utilisateur recevra un avertissement si la stratégie a été enfreinte et l‘action de correction configurée sera appliquée.

Principales fonctionnalités de CylanceAVERT

Fonctionnalité	Description
Analyse des données sensibles	CylanceAVERT peut analyser les fichiers chargés sur des clés USB, des navigateurs Internet et des pièces jointes d‘e-mail, ainsi que le contenu du corps d‘un e-mail pour rechercher des données d‘entreprise que l‘administrateur a définies comme sensibles dans les politiques de protection des informations. Une notification par e-mail sera envoyée pour les évènements d‘exfiltration de données.
Stratégies de protection des informations	Vous pouvez spécifier les conditions qui doivent être remplies pour déclencher la violation de stratégie, les domaines autorisés pour la stratégie et les actions à entreprendre en cas de violation d‘une stratégie. Pour plus d‘informations, consultez Gérer des stratégies de protection des informations dans le Guide de configuration de Cylance Endpoint Security.
Évènements CylanceAVERT	Vous pouvez créer des stratégies de protection des informations pour spécifier les données et les conditions qui doivent être remplies pour déclencher une violation de stratégie, ainsi que les emplacements où appliquer la stratégie, les activités à surveiller et les mesures correctives à prendre en cas de violation d‘une stratégie. Pour plus d‘informations, consultez Évènements CylanceAVERT du Guide de configuration de Cylance Endpoint Security.
Paramètres de protection des données	Vous pouvez utiliser les paramètres de protection des informations pour configurer les données sensibles qu‘ils souhaitent surveiller en ajoutant des modèles et des types de données à utiliser dans une stratégie de protection des informations. Les administrateurs peuvent également définir les domaines de navigateur et de messagerie qui seront autorisés et approuvés, gérer les preuves qu‘ils souhaitent collecter pour les évènements d‘exfiltration de données et spécifier la durée de disponibilité des preuves. Les adresses e-mail spécifiées peuvent également recevoir des notifications d‘évènements d‘exfiltration de données. Pour plus d‘informations, consultez Définir le contenu sensible à l‘aide des paramètres de protection de l‘information dans le Guide de configuration de Cylance Endpoint Security.

Fonctionnalité	Description
Inventaire des fichiers	L'inventaire des fichiers CylanceAVERT crée un enregistrement de tous les fichiers sensibles d'une organisation par le biais d'un processus de suivi des fichiers. Pour plus d'informations, consultez Utiliser l'inventaire des fichiers pour identifier les fichiers sensibles dans le Guide d'administration Cylance Endpoint Security.
Casier de preuves	Vous pouvez utiliser le casier de preuves pour afficher les détails des fichiers qui ont été impliqués dans des évènements d'exfiltration et télécharger les fichiers sur leur stockage local à des fins d'audit. Pour plus d'informations, consultez Utiliser le casier de preuves pour voir les détails de l'évènement d'exfiltration dans le Guide d'administration Cylance Endpoint Security.

Architecture : CylanceAVERT



Élément	Description
CylanceAVERT	CylanceAVERT empêche la perte de données sensibles d'être exfiltrée par le biais d'e-mails et de pièces jointes, de téléchargements de navigateurs et de terminaux USB.
Casier de preuves	Le casier de preuves est une zone de stockage de fichiers privée qui stocke les fichiers impliqués dans des évènements d'exfiltration non autorisés pour une inspection ultérieure par les administrateurs.
Console de gestion	La console de gestion basée sur le cloud vous permet de définir les données sensibles de l'entreprise que vous souhaitez surveiller et protéger, de gérer les stratégies utilisateur pour spécifier les conditions à respecter pour déclencher un évènement d'exfiltration, d'afficher les fichiers sensibles de votre organisation, et afficher divers évènements liés aux menaces pour l'évaluation et la résolution des risques.
Terminaux avec CylanceAVERT et CylancePROTECT	CylancePROTECT Desktop doit être installé sur le point de terminaison pour utiliser la fonctionnalité CylanceAVERT. CylanceAVERT prend en charge Windows 10 et 11.

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