Dell Threat Defense

Guide d'installation et d'administration

Basé sur Cylance

v17.11.06

2017-11-06

Table des matières

PRÉSENTATION 6
Fonctionnement 6
À propos de ce guide 6
CONSOLE 7
Connexion 7
Stratégie de périphérique 7
Actions de fichier 8
Paramètres de protection 9
Journaux d'agent 10
Meilleures pratiques pour les stratégies 10
Zones 11
Propriétés des zones 12
Règle de zone 13
Liste Périphériques de la zone 15
Meilleures pratiques de gestion des zones 15
Gestion des utilisateurs 17
Options liées au réseau 17
Pare-feu 18
Proxy 18
Périphériques 19
Gestion des périphériques 19
Menaces et activités 19
Périphériques en double 21
Mise à jour de l'agent 21
Tableau de bord 22
Protection – Menaces 24
Type de fichier 24
Score Cylance 24
Affichage des informations de menace 24
Traitement des menaces 26
Traitement des menaces sur un périphérique spécifique 27
Traitement des menaces au niveau global 27
Protection – Contrôle des scripts 28
Liste globale 28

Liste de confiance par certificat ... 29
Profil ... 30
Mon compte ... 30
Journaux d'audit ... 31
Paramètres ... 31
APPLICATION ... 31
Agent Threat Defense ... 31
Agent Windows ... 32
Configuration système requise ... 32
Installation de l'agent – Windows ... 33
Paramètres d'installation Windows ... 33
Installation de l'agent Windows avec Wyse Device Manager (WDM) ... 34
Mise en quarantaine à l'aide de la ligne de commande ... 36
Désinstallation de l'agent ... 36
Agent macOS ... 37
Configuration système requise ... 37
Installation de l'agent - macOS ... 38
Paramètres d'installation macOS ... 38
Installation de l'agent ... 39
Désinstallation de l'agent ... 40
Service d'agent ... 40
Menu Agent ... 41
Activation des options avancées de l'interface utilisateur de l'agent ... 42
Machines virtuelles ... 43
Désinstallation protégée par un mot de passe ... 43
Pour créer un mot de passe de désinstallation ... 43
Intégrations ... 44
Syslog/SIEM ... 44
Authentification personnalisée ... 45
Rapport des données de menace ... 46
DÉPANNAGE ... 46
Support ... 47
Paramètres d'installation ... 47
Problèmes de performances ... 47
Problèmes de mise à jour, d'état et de connexion ... 47
Activation des journaux de débogage ... 47

Incompatibilités de Contrôle des scripts 47
ANNEXE A : GLOSSAIRE 49
ANNEXE B : GESTION DES EXCEPTIONS 49
Fichiers 49
Scripts 50
Certificats 50
ANNEXE C : AUTORISATIONS UTILISATEUR 50
ANNEXE D : FILTRE D'ÉCRITURE BASÉ SUR DES FICHIERS 51

PRÉSENTATION

Dell Threat Defense, basé sur Cylance, détecte et bloque les programmes malveillants avant qu'ils n'affectent les périphériques. Cylance utilise une approche mathématique de l'identification des programmes malveillants, qui consiste à utiliser des techniques d'apprentissage machine au lieu de signatures réactives, ou de systèmes de fichiers de confiance ou de « sandbox ». Cette approche rend inoffensifs les nouveaux programmes malveillants, virus et bots, ainsi que leurs futures variantes. Threat Defense analyse l'exécution potentielle des fichiers afin de détecter les programmes malveillants dans le système d'exploitation.

Ce guide décrit l'utilisation de la console Threat Defense, l'installation de l'agent Threat Defense et la procédure de configuration de ces deux modules.

Fonctionnement

Threat Defense comprend un petit agent, qui s'installe sur chacun des hôtes qui communique avec la console dans le cloud. L'agent détecte et prévient les programmes malveillants sur l'hôte à l'aide de modèles mathématiques qui ont été testés. Il n'a pas besoin d'être connecté au cloud en continu, ni de recevoir constamment des mises à jour des signatures, et il fonctionne à la fois sur les réseaux ouverts et les réseaux isolés. Threat Defense évolue avec les changements du paysage des menaces virales. Par un apprentissage constant sur d'énormes volumes de données du monde réel, Threat Defense anticipe les actions des pirates.

- **Menace** : signale qu'une menace a été téléchargée sur le périphérique ou qu'il y a eu tentative d'attaque par exploitation (Exploit).
- **Détection des menaces** : méthode appliquée par l'agent Threat Defense pour identifier les menaces.
    - **Analyse des processus** : analyse les divers processus exécutés sur le périphérique.
    - **Contrôle de l'exécution** : analyse les processus uniquement lors de leur exécution. Cela inclut tous les fichiers exécutés au démarrage, ceux qui sont configurés pour exécution automatique et ceux qui sont exécutés manuellement par l'utilisateur.
- **Analyse** : méthode permettant d'identifier les fichiers comme dangereux ou sûrs.
    - **Recherche dans le cloud des scores de menaces** : modèle mathématique exécuté dans le cloud pour attribuer un score aux fichiers.
    - **Local** : modèle mathématique inclus avec l'agent. Il permet d'effectuer une analyse lorsque le périphérique n'est pas connecté à Internet.
- **Action** : opération que l'agent réalise lorsqu'un fichier est identifié comme une menace.
    - **Global** : vérifie les paramètres de stratégie, dont *Quarantaine globale* et *Listes de confiance*.
    - **Local** : vérifie les fichiers manuellement *mis en quarantaine* ou *ignorés*.

À propos de ce guide

Dell recommande aux utilisateurs de se familiariser avec la console dans le cloud avant d'installer l'agent sur les points de terminaison. La compréhension du mode de gestion des points de terminaison facilite leur protection et leur maintenance. Ce flux de travail n'est qu'une recommandation. Les utilisateurs peuvent aborder le déploiement dans leur environnement selon une approche qui a du sens pour eux.

Exemple : les zones vous aident à regrouper les périphériques au sein de l'entreprise. Par exemple, configurez une zone dotée d'une règle de zone qui ajoute automatiquement les nouveaux périphériques à une zone spécifique en fonction des critères sélectionnés (Système d'exploitation, Nom de périphérique ou Nom de domaine, par exemple).

Remarque : les instructions d'installation de l'agent sont présentées après les détails concernant les stratégies et les zones. Les utilisateurs peuvent commencer par installer l'agent, si nécessaire.

CONSOLE

La console Threat Defense est un site Web auquel le système se connecte pour afficher les informations de menaces pertinentes pour l'entreprise. La console facilite l'organisation des périphériques en groupes (zones), la configuration des actions à exécuter lorsque des menaces sont détectées sur un périphérique (stratégie) et le téléchargement des fichiers d'installation (agent).

La console Threat Defense prend en charge les langues suivantes.

Français	Allemand	Italien	Japonais
Portugais (ibérique)	Coréen	Espagnol	Portugais (brésilien)

Tableau 1 : Langues prises en charge par la console Threat Defense

Connexion

Lors de l'activation de votre compte, vous recevez un e-mail contenant vos informations de connexion à la console Threat Defense. Cliquez sur le lien figurant dans l'e-mail pour accéder à la page de connexion, ou utilisez les adresses suivantes :

- Amérique du Nord : http://dellthreatdefense.com
- Europe : http://dellthreatdefense-eu.cylance.com

Stratégie de périphérique

Une stratégie définit la manière dont l'agent traite les programmes malveillants qu'il rencontre. Par exemple, le programme malveillant peut être automatiquement *mis en quarantaine* ou ignoré s'il se trouve dans un dossier spécifique. Chaque périphérique doit comporter une stratégie et vous ne pouvez appliquer qu'une seule stratégie à chaque périphérique. En limitant les stratégies à une seule par périphérique, le système évite les conflits de fonctions (par exemple, vous évitez de bloquer un fichier alors qu'il doit être autorisé pour ce périphérique spécifique). Le périphérique est placé sous Stratégie par défaut si aucune stratégie ne lui est attribuée.

Seule la fonction Contrôle de l'exécution est activée pour Stratégie par défaut ; elle analyse les processus uniquement lors de leur exécution. Cela offre une protection de base pour le périphérique, ne devrait pas interrompre le fonctionnement de ce périphérique et vous laisse le temps de tester les fonctions de la stratégie avant de la déployer dans l'environnement de production.

Pour ajouter une stratégie

1. Connectez-vous à la console (http://dellthreatdefense.com) en tant qu'administrateur. Seuls les administrateurs peuvent créer des stratégies.
2. Sélectionnez **Paramètres > Stratégie de périphérique**.
3. Cliquez sur **Ajouter une nouvelle stratégie**.
4. Entrez un nom de stratégie et sélectionnez des options de stratégie.
5. Cliquez sur **Créer**.

Actions de fichier

PARAMÈTRES > Stratégie de périphérique > [sélectionnez une stratégie] > Actions de fichier

La zone Actions de fichier offre différentes options permettant de manipuler les fichiers que Threat Defense a identifiés comme *dangereux* ou *anormaux*.

Conseil : pour en savoir plus sur la classification des fichiers comme *dangereux* ou *anormaux*, voir la section Protection – Menaces.

Mise en quarantaine automatique avec contrôle de l'exécution

Cette fonction *met en quarantaine* ou bloque le fichier *dangereux* ou *anormal* afin de l'empêcher de s'exécuter. La *mise en quarantaine* d'un fichier le déplace de son emplacement d'origine vers le répertoire de *quarantaine*, **`C:\ProgramData\Cylance\Desktop\q`**.

Certains programmes malveillants sont conçus pour déposer d'autres fichiers dans certains répertoires. Le programme malveillant continue à procéder ainsi jusqu'à ce que le fichier soit déplacé avec succès. Threat Defense modifie le fichier déplacé afin qu'il ne puisse pas s'exécuter, ce qui empêche ce type de programme malveillant de continuer à déposer le fichier supprimé.

Conseil : Dell vous recommande de tester la fonction *Quarantaine auto* sur un petit nombre de terminaux avant de l'appliquer à votre environnement de production. Observez bien les résultats du test pour vous assurer qu'aucune application essentielle à vos activités n'est bloquée lors de l'exécution.

Téléchargement auto

Dell recommande aux utilisateurs d'activer la fonction Téléchargement auto pour les fichiers *dangereux* ou *anormaux*. Threat Defense télécharge automatiquement tous les fichiers *dangereux* ou *anormaux* sur le cloud Cylance Infinity, qui les analyse de manière plus approfondie et fournit davantage d'informations à leur propos.

Threat Defense télécharge et analyse uniquement les fichiers Portable Executable (PE) inconnus. Si le même fichier inconnu est découvert sur plusieurs périphériques de l'entreprise, Threat Defense ne télécharge qu'un seul fichier pour analyse, et non pas un fichier par périphérique.

Liste de confiance de la stratégie

Ajoutez à cette liste les fichiers considérés comme sûrs, au niveau de la stratégie. L'agent n'applique aucune action de suppression des menaces aux fichiers de cette liste.

Pour en savoir plus sur la gestion des exceptions de fichiers (*mis en quarantaine* ou *ajoutés à la liste de confiance*) à différents niveaux (*Local*, *Stratégie* ou *Global*), voir Annexe B : Gestion des exceptions.

1. Connectez-vous à la console (http://dellthreatdefense.com) en tant qu'administrateur. Seuls les administrateurs peuvent créer des stratégies.
2. Sélectionnez **Paramètres > Stratégie de périphérique**.
3. Ajoutez une nouvelle stratégie ou modifiez une stratégie existante.
4. Cliquez sur **Ajouter un fichier**, sous *Liste de confiance de la stratégie*.
5. Saisissez les informations de hachage **SHA256**. (Facultatif) Indiquez la valeur MD5 et le nom du fichier si vous les connaissez.
6. Sélectionnez une **catégorie** pour faciliter l'identification du rôle de ce fichier.
7. Indiquez la raison pour laquelle vous ajoutez ce fichier à la *liste de confiance de la stratégie*.
8. Cliquez sur **Envoyer**.

Paramètres de protection

PARAMÈTRES > Stratégie de périphérique > [sélectionnez une stratégie] > Paramètres de protection

Contrôle de l'exécution

Threat Defense surveille toujours l'exécution de processus malveillants, et émet une alerte chaque fois qu'un élément marqué comme *dangereux* ou *anormal* tente de s'exécuter.

Interdire l'arrêt du service depuis le périphérique

Si cette option est sélectionnée, le service Threat Defense ne peut pas être arrêté manuellement ni par un autre processus.

Copier les échantillons de programme malveillant

Permet de spécifier un partage réseau où copier des échantillons de programme malveillant. Cela permet aux utilisateurs d'effectuer leur propre analyse des fichiers que Threat Defense identifie comme *dangereux* ou *anormaux*.

- Prend en charge les partages réseau CIFS/SMB.
- Spécifiez un seul partage réseau. Exemple : **`c:\test`**.
- Tous les fichiers qui répondent aux critères sont copiés vers le partage réseau, y compris les doublons. Aucun test d'unicité n'est effectué.
- Les fichiers ne sont pas compressés.
- les fichiers ne sont pas protégés par mot de passe.

AVERTISSEMENT : LES FICHIERS NE SONT PAS PROTEGES PAR MOT DE PASSE. SOYEZ PRUDENT AFIN DE NE PAS EXECUTER PAR INADVERTANCE LE FICHIER MALVEILLANT.

Contrôle des scripts

Le contrôle des scripts protège les périphériques en empêchant l'exécution des scripts Active Script et PowerShell malveillants.

1. Connectez-vous à la console (http://dellthreatdefense.com).
2. Sélectionnez **Paramètres > Stratégie de périphérique**.
3. Sélectionnez une stratégie, puis cliquez sur **Paramètres de protection**.
4. Cochez la case correspondante pour activer l'option **Contrôle des scripts**.
    a. **Alerte** : surveille les scripts exécutés dans votre environnement. Recommandé lors du déploiement initial.
    b. **Bloquer** : autorise l'exécution des scripts uniquement à partir de dossiers spécifiques. Utilisez cette option après l'avoir testée en mode Alerte.
    c. **Approuver les scripts dans ces dossiers (et leurs sous-dossiers)** : vous devez indiquer des exclusions de dossier en entrant le chemin relatif de chaque dossier.
    d. **Bloquer l'utilisation de la console PowerShell** : empêche le lancement de la console PowerShell. Cette option fournit une sécurité supplémentaire en empêchant l'utilisation de messages d'une ligne PowerShell.

    Remarque : si le script lance la console PowerShell alors que l'option Contrôle des scripts est configurée pour bloquer son exécution, le script échoue. Il est recommandé aux utilisateurs de modifier leurs scripts pour invoquer les scripts PowerShell, et non la console PowerShell.
5. Cliquez sur **Enregistrer**.

Journaux d'agent

PARAMÈTRES > Stratégie de périphérique > [sélectionnez une stratégie] > Journaux d'agent

Active les journaux d'agent dans la console pour qu'il soit possible de télécharger ces fichiers journaux et de les afficher dans la console.

1. Connectez-vous à la console (http://dellthreatdefense.com).
2. Sélectionnez **Paramètres > Stratégie de périphérique**.
3. Sélectionnez une stratégie, puis cliquez sur **Journaux de l'agent**. Vérifiez que le périphérique sélectionné pour les fichiers journaux est bien associé à cette stratégie.
4. Sélectionnez **Activer le téléchargement auto des fichiers journaux**, puis cliquez sur **Exécuter**.
5. Cliquez sur l'onglet **Périphériques** et sélectionnez un périphérique.
6. Cliquez sur **Journaux de l'agent**. Les fichiers journaux s'affichent.
7. Cliquez sur un journal. Le nom du fichier journal correspond à sa date de création.

Meilleures pratiques pour les stratégies

Lors de la création initiale des stratégies, Dell vous recommande d'implémenter les fonctions de stratégie phase par phase, afin de vous assurer qu'elles n'ont pas d'impact sur les performances et les opérations. Créez les nouvelles stratégies en activant de plus en plus de fonctions au fur et à mesure que vous vous familiarisez avec le fonctionnement de Threat Defense dans votre environnement.

1. Lors de la création des stratégies initiales, activez uniquement l'option **Téléchargement auto**.
    a. L'agent utilise Contrôle de l'exécution et Surveillance des processus pour analyser uniquement les processus en cours d'exécution.

    Cela inclut tous les fichiers exécutés au démarrage, ceux qui sont configurés pour exécution automatique et ceux qui sont exécutés manuellement par l'utilisateur.

    L'agent envoie uniquement des alertes à la console. Aucun fichier n'est bloqué ni *mis en quarantaine*.

    b. Consultez la console pour voir s'il existe des alertes de menace.

    L'objectif est de repérer les applications ou les processus dont l'exécution est nécessaire sur le point de terminaison, mais qui sont considérés comme des menaces (identifiés comme *anormaux* ou *dangereux*).

    Configurez une stratégie ou un paramètre de console pour *autoriser* ces éléments à s'exécuter, le cas échéant (par exemple, *exclure* les dossiers dans une stratégie, *ignorer* les fichiers pour un périphérique donné ou ajouter les fichiers à la *liste de confiance*).

    c. Utilisez cette stratégie initiale pendant une journée afin d'autoriser l'exécution des applications et processus généralement utilisés sur le périphérique ; ils seront également analysés.

IMPORTANT : certains processus et applications exécutés périodiquement sur un périphérique (une fois par mois, par exemple) peuvent être considérés comme une menace. C'est à vous de décider si vous préférez exécuter cette fonction pendant la stratégie d'origine ou surveiller le périphérique lors de son exécution, selon la planification définie.

2. Sous Paramètres de protection, activez l'option **Arrêter les processus en cours d'exécution dangereux** une fois le contrôle d'exécution et la surveillance des processus terminés.

    L'option Arrêter les processus en cours d'exécution dangereux et tous leurs sous-processus permet d'arrêter tous les processus (et sous-processus), quel que soit leur état, si une menace est détectée (EXE ou MSI).

3. Sous Actions de fichier, activez l'option **Quarantaine auto**.

   Quarantaine auto déplace les fichiers malveillants dans le dossier de *quarantaine*.

4. Sous Paramètres de protection, activez l'option **Contrôle des scripts**.

   Le contrôle des scripts protège les utilisateurs des scripts malveillants en empêchant leur exécution sur les périphériques.

   Les utilisateurs peuvent approuver l'exécution des scripts pour des dossiers spécifiques.

   Vous devez indiquer les exclusions de dossier Contrôle des scripts en entrant le chemin relatif du dossier (par exemple, **`\Cases\Scripts`**).

Zones

Une zone permet d'organiser et de gérer les périphériques. Par exemple, vous pouvez regrouper les périphériques par site géographique ou par fonction. S'il existe un groupe de périphériques critiques, vous pouvez les regrouper en une zone et leur attribuer une priorité élevée. De plus, vous appliquez des stratégies au niveau de la zone, si bien qu'il est possible de regrouper des périphériques en une zone sur la base de la stratégie qui leur est appliquée.

Chaque entreprise possède une zone par défaut (périphériques sans zone), accessible uniquement pour les administrateurs. Les nouveaux périphériques sont placés sous Sans zone, sauf si vous avez défini des règles de zone pour associer automatiquement les périphériques à des zones.

Les gestionnaires de zone et les utilisateurs peuvent être associés à des zones, ce qui leur permet d'afficher la configuration de ces zones. Cela permet également aux gestionnaires de zone et aux utilisateurs d'accéder aux périphériques dont ils sont responsables. Vous devez créer au moins une zone, et autoriser toutes les personnes dotées d'un rôle Gestionnaire de zone ou Utilisateur à l'afficher.

Un périphérique peut appartenir à plusieurs zones mais vous ne pouvez appliquer qu'une seule stratégie à chaque périphérique. La mise en place de plusieurs zones permet davantage de flexibilité dans le mode de regroupement des périphériques. En limitant les stratégies à une seule par périphérique, le système évite les conflits de fonctions (par exemple, vous évitez de bloquer un fichier alors qu'il doit être *autorisé* pour le périphérique).

Un périphérique peut appartenir à plusieurs zones pour différentes raisons :

- Vous ajoutez manuellement ce périphérique à plusieurs zones.
- Le périphérique est conforme aux règles de plusieurs zones.
- Le périphérique résidait déjà dans une zone mais il devient conforme aux règles d'une autre zone.

Pour connaître les méthodes d'utilisation recommandées des zones, voir Meilleures pratiques de gestion des zones.

Pour ajouter une zone

1. Connectez-vous à la console (http://dellthreatdefense.com) en tant qu'administrateur. Seuls les administrateurs peuvent créer des zones.
2. Cliquez sur **Zones**.
3. Cliquez sur **Ajouter une nouvelle zone**.
4. Entrez un nom de zone, sélectionnez une stratégie et choisissez une valeur. Chaque zone doit être associée à une stratégie. La valeur détermine la priorité de la zone.
5. Cliquez sur **Enregistrer**.

Pour ajouter des périphériques à une zone

1. Connectez-vous à la console (http://dellthreatdefense.com) à l'aide d'un compte d'administrateur ou de gestionnaire de zone.
2. Cliquez sur **Zones**.
3. Cliquez sur une zone de la *liste des zones*. Les périphériques se trouvant actuellement dans la zone sélectionnée s'affichent dans la *liste des périphériques de la zone*, au bas de la page.
4. Cliquez sur **Ajouter des périphériques à la zone**. Une liste de périphériques s'affiche.
5. Sélectionnez tous les périphériques à ajouter à la zone, puis cliquez sur **Enregistrer**. Vous pouvez éventuellement sélectionner l'option **Appliquer la stratégie de zone aux périphériques sélectionnés**. L'ajout d'un périphérique à une zone n'applique pas automatiquement la stratégie de zone, car la zone concernée peut servir à organiser les périphériques et pas à gérer la stratégie pour ces périphériques.

Pour supprimer une zone

1. Connectez-vous à la console (http://dellthreatdefense.com) en tant qu'administrateur. Seuls les administrateurs peuvent supprimer des zones.
2. Cliquez sur **Zones**.
3. Cochez les cases des zones à supprimer.
4. Cliquez sur **Supprimer**.
5. Cliquez sur **Oui** dans le message vous invitant à confirmer la suppression de la zone sélectionnée.

Propriétés des zones

Vous pouvez modifier les propriétés de zone selon vos besoins.

À propos de la priorité des zones

Vous pouvez attribuer aux zones différents niveaux de priorité (Faible, Normal ou Élevé), qui déterminent la pertinence ou l'importance des périphériques de chaque zone. Dans différentes sections du tableau de bord, les périphériques sont affichés dans l'ordre de priorité pour vous aider à identifier les périphériques à traiter immédiatement.

Vous pouvez définir la priorité lors de la création de la zone ou modifier la zone ultérieurement pour changer son ordre de priorité.

Pour modifier les propriétés des zones

1. Connectez-vous à la console (http://dellthreatdefense.com) en tant qu'administrateur ou gestionnaire de zone.
2. Cliquez sur **Zones**.
3. Cliquez sur une zone de la *liste des zones*.
4. Pour renommer la zone, saisissez un nouveau nom dans le champ **Nom**.
5. Pour changer de stratégie, sélectionnez-en une autre dans le menu déroulant **Stratégie.**
6. Faites votre choix entre les valeurs **Faible**, **Normal** et **Élevé**.
7. Cliquez sur **Enregistrer**.

Règle de zone

Vous pouvez associer automatiquement les périphériques à une zone sur la base de certains critères. Cette automatisation s'avère très utile si vous ajoutez un grand nombre de périphériques à des zones. Lorsque vous ajoutez un nouveau périphérique qui satisfait la règle d'une zone, il est automatiquement associé à cette zone. Si l'option **Appliquer maintenant à tous les périphériques sélectionnés** est sélectionnée, tous les périphériques prédéfinis sont ajoutés à cette zone.

Remarque : les règles de zone ajoutent automatiquement des périphériques à une zone, mais elles ne peuvent pas les en retirer. La modification de l'adresse IP ou du nom d'hôte d'un périphérique ne retire pas ce périphérique d'une zone. Vous devez retirer manuellement les périphériques de leur zone.

Il existe une option permettant d'appliquer la stratégie de zone aux périphériques qui ont été ajoutés à la zone en question parce qu'ils correspondaient à la règle de zone. Cela signifie que la stratégie existante du périphérique est remplacée par la stratégie de zone spécifiée. Soyez prudent lorsque vous appliquez automatiquement une stratégie sur la base de la règle de zone. En effet, si vous ne gérez pas correctement cette fonction, un périphérique peut se voir attribuer la mauvaise stratégie simplement parce qu'il correspond à une règle de zone.

Consultez la page Détails du périphérique de la console pour connaître la stratégie appliquée au périphérique concerné.

Pour ajouter une règle de zone

1. Connectez-vous à la console (http://dellthreatdefense.com) en tant qu'administrateur ou gestionnaire de zone.
2. Cliquez sur **Zones**, puis sélectionnez une zone dans la *liste des zones*.
3. Cliquez sur **Créer une règle** sous Règle de zone.
4. Spécifiez les critères de la zone sélectionnée. Cliquez sur le signe plus pour ajouter des conditions. Cliquez sur le signe moins pour supprimer une condition.
5. Cliquez sur **Enregistrer**.

Critères de règle de zone

- **Lorsqu'un nouveau périphérique est ajouté à l'organisation** : tous les nouveaux périphériques ajoutés à l'entreprise qui correspondent à la règle de zone sont ajoutés à la zone en question.
- **Lorsqu'un attribut d'un périphérique a changé** : lorsque les attributs d'un périphérique existant changent et que ce périphérique devient conforme à la règle de zone, ce périphérique existant est ajouté à la zone.
- **Adresse IPv4 incluse à la plage** : entrez une plage d'adresses IPv4.
- **Nom du périphérique** :
    - Commence par : indique les caractères par lesquels les noms de périphérique doivent commencer.
    - Contient : indique la chaîne que les noms de périphérique doivent contenir, quelle que soit sa position dans le nom.
    - Finit par : indique les caractères par lesquels les noms de périphérique doivent se terminer.
- **Système d'exploitation** :
    - Est : le système d'exploitation doit être identique à celui qui est sélectionné ici.
    - N'est pas : le système d'exploitation doit être différent de celui qui est sélectionné ici. Par exemple, si la seule règle de zone indique que le système d'exploitation doit être différent de Windows 8, les périphériques utilisant tous les autres systèmes d'exploitation, y compris non-Windows, sont ajoutés à cette zone.

- **Nom de domaine** :
    - Commence par : indique les caractères par lesquels le nom de domaine doit commencer.
    - Contient : indique la chaîne que le nom de domaine doit contenir, quelle que soit sa position dans le nom.
    - Finit par : indique les caractères par lesquels le nom de domaine doit se terminer.
- **Nom distinctif** :
    - Commence par : indique les caractères par lesquels le nom distinctif doit commencer.
    - Contient : indique la chaîne que le nom distinctif doit contenir, quelle que soit sa position dans le nom.
    - Finit par : indique les caractères par lesquels le nom distinctif doit se terminer.
- **Membre de (LDAP)** :
    - Est : la zone Membre de (Groupe) doit correspondre à la valeur entrée ici.
    - Contient : la zone Membre de (Groupe) doit contenir la valeur entrée ici.
- **Les conditions suivantes sont réunies** :
    - Toutes : toutes les conditions de la règle de zone doivent être satisfaites pour que le périphérique soit ajouté.
    - N'importe laquelle : au moins une condition de la règle de zone doit être satisfaite pour que le périphérique soit ajouté.
- **Application de la stratégie de zone** :
    - Ne pas appliquer : ne pas appliquer la stratégie de zone lorsque des périphériques sont ajoutés à la zone.
    - Appliquer : appliquer la stratégie de zone lorsque des périphériques sont ajoutés à la zone.

      Avertissement : l'application automatique d'une stratégie de zone peut avoir un impact négatif sur certains des périphériques du réseau. Appliquez automatiquement la stratégie de zone *uniquement* lorsqu'il est certain que la stratégie de zone trouvera *uniquement* les périphériques auxquels cette stratégie de zone spécifique *doit* être appliquée.
- **Appliquer maintenant à tous les périphériques existants** : applique la règle de zone à tous les périphériques de l'entreprise. Cette option n'applique pas la stratégie de zone.

À propos des noms distinctifs (DN)

Voici des informations que vous devez connaître à propos des noms distinctifs (DN) pour les utiliser dans les règles de zone.

- Les caractères génériques sont interdits, mais la condition « Contient » donne pratiquement le même résultat.
- Les erreurs de DN et les exceptions liées à l'agent sont consignées dans les fichiers journaux.
- Si l'agent trouve les informations de DN sur le périphérique, ces informations sont automatiquement envoyées à la console.
- Lorsque vous ajoutez un nom distinctif (DN), veillez à utiliser le format correct, comme suit.
    - Exemple : CN=JDoe,OU=Sales,DC=dell,DC=COM
    - Exemple : OU=Demo,OU=SEngineering,OU=Sales

Liste Périphériques de la zone

La *liste Périphériques de la zone* affiche tous les périphériques attribués à cette zone. Les périphériques peuvent appartenir à plusieurs zones. Utilisez l'option **Exporter** pour télécharger un fichier CSV contenant des informations pour tous les périphériques de la *liste Périphériques de la zone*.

Remarque : si l'autorisation d'affichage d'une zone n'a pas été attribuée et si l'utilisateur clique quand même sur le lien vers la zone dans la colonne Zones, la page Ressource introuvable s'affiche.

Meilleures pratiques de gestion des zones

Considérez les zones comme des balises, car chaque périphérique peut appartenir à plusieurs zones (porter plusieurs balises). Bien qu'il n'existe aucune restriction concernant le nombre de zones que vous pouvez créer, les meilleures pratiques recommandent de créer 3 zones pour le test, les stratégies et la granularité des rôles d'utilisateur au sein de l'entreprise.

Ces 3 zones sont les suivantes :

- Gestion des mises à jour
- Gestion des règles
- Gestion de l'accès basé sur les rôles

Organisation des zones pour la gestion des mises à jour

Les zones sont souvent utilisées pour faciliter la gestion des mises à jour de l'agent. Threat Defense prend en charge la version la plus récente de l'agent, ainsi que la précédente. Cela permet à l'entreprise de gérer des périodes de gel des changements et de tester entièrement les nouvelles versions de l'agent.

Voici 3 types de zone suggérés pour diriger et spécifier les phases de test et de production de l'agent :

- **Zone de mise à jour – Groupe de test** : cette zone doit contenir des périphériques de test réellement représentatifs des périphériques de l'entreprise (et des logiciels qui sont utilisés sur ces périphériques). Cela permet de tester la version la plus récente de l'agent et garantit que le déploiement de cet agent sur les périphériques de l'environnement de production ne va pas perturber les processus d'entreprise.
- **Zone de mise à jour – Groupe pilote** : cette zone peut être utilisée comme zone de test secondaire ou comme zone de production secondaire. S'il s'agit d'une zone de test secondaire, elle peut permettre de tester le nouvel agent sur un groupe de périphériques plus étendu avant le déploiement dans l'environnement de production. En tant que zone de production secondaire, elle vous permet d'utiliser deux versions différentes de l'agent, à condition de définir deux zones de production distinctes.
- **Zone de mise à jour – Production** : la plupart des périphériques doivent se trouver dans la zone conçue pour l'environnement de production.

Remarque : pour mettre à jour l'agent dans la zone Production, voir la section Mise à jour de l'agent.

Ajout d'une zone de test ou pilote

1. Connectez-vous à la console (http://dellthreatdefense.com) à l'aide d'un compte d'administrateur ou de gestionnaire de zone.
2. Sélectionnez **Paramètres > Mise à jour de l'agent**.
3. Pour les zones de test ou pilotes :
    a. Cliquez sur **Sélectionner les zones de test** ou **Sélectionner les zones pilotes**.
    b. Sélectionnez une zone.

    Si la zone Production est définie sur **Mise à jour auto**, les zones de test et zones pilotes ne sont pas disponibles. Pour activer les zones de test et zones pilotes, remplacez l'option Mise à jour auto de la zone Production par une autre option.

4. Cliquez sur **Sélectionnez la version**.
5. Sélectionnez la version de l'agent à appliquer à la zone de test ou pilote.
6. Cliquez sur **Appliquer**.

Organisation des zones pour la gestion des stratégies

Un autre ensemble de zones peut vous aider à appliquer différentes stratégies aux divers types de point de terminaison. Voici quelques exemples :

- Zone de stratégie – Postes de travail
- Zone de stratégie – Postes de travail – Exclusions
- Zone de stratégie – Serveurs
- Zone de stratégie – Serveurs – Exclusions
- Zone de stratégie – Direction – Protection renforcée

Dell vous suggère d'appliquer une stratégie par défaut à tous les périphériques de cette zone de stratégie dans l'une de ces zones. Attention à ne pas placer un périphérique dans plusieurs zones de stratégie, car cela créerait un conflit pour l'application de la stratégie. Souvenez-vous également qu'un moteur de règle de zone peut vous aider à organiser automatiquement les hôtes sur la base de l'adresse IP, du nom d'hôte, du système d'exploitation ou du domaine.

Organisation des zones pour la gestion de l'accès basé sur les rôles

L'accès basé sur les rôles (RBAC) permet de limiter l'accès d'un utilisateur de la console au seul sous-ensemble de périphériques qu'il est chargé de gérer. Vous pouvez répartir les périphériques par plage d'adresses IP, par nom d'hôte, par système d'exploitation ou par domaine. Vous pouvez également créer des groupes sur la base de l'emplacement géographique, du type ou des deux.

Exemple :

- Zone RBAC – Postes de travail – Europe
- Zone RBAC – Serveurs – Asie
- Zone RBAC – Tapis rouge (Direction)

À l'aide des exemples de zones ci-dessus, un gestionnaire de zone peut être attribué à *Zone RBAC – Bureaux – Europe* et avoir uniquement accès aux périphériques se trouvant dans cette zone. Si l'utilisateur Gestionnaire de zone tente d'afficher les autres zones, il reçoit un message d'erreur qui lui précise qu'il n'a pas l'autorisation d'affichage requise. Bien qu'un périphérique puisse se trouver dans plusieurs zones et que le gestionnaire de zone soit autorisé à afficher ce périphérique, il n'est pas autorisé à l'afficher dans les autres zones dont ce périphérique est membre ; le message d'erreur apparaît.

Dans d'autres sections de la console, comme le tableau de bord, le gestionnaire de *Zone RBAC – Bureaux – Europe* serait également limité aux menaces et autres informations associées à cette zone ou aux périphériques qui y sont affectés.

Les mêmes restrictions s'appliquent aux comptes Utilisateur associés à une zone.

Gestion des utilisateurs

Les administrateurs disposent d'autorisations globales. Ils peuvent ajouter ou supprimer des utilisateurs, associer des utilisateurs à des zones (en tant qu'utilisateur ou gestionnaire de zone), ajouter ou supprimer des périphériques, créer des stratégies et créer des zones. Les administrateurs peuvent également supprimer définitivement de la console des utilisateurs, des périphériques, des stratégies et des zones.

Les comptes Utilisateur et Gestionnaire de zone ont un accès limité et disposent uniquement des privilèges liés à la zone qui leur est attribuée. Cela s'applique aux périphériques affectés à la zone, aux menaces détectées sur ces périphériques et aux informations du tableau de bord.

Pour consulter la liste complète des autorisations associées à chaque type d'utilisateur, voir Annexe C : Autorisations utilisateur.

Pour ajouter des utilisateurs

1. Connectez-vous à la console (http://dellthreatdefense.com) en tant qu'administrateur. Seuls les administrateurs peuvent créer des utilisateurs.
2. Sélectionnez **Paramètres > Gestion des utilisateurs**.
3. Entrez l'adresse e-mail de l'utilisateur.
4. Sélectionnez un rôle dans la liste déroulante Rôle.
5. Lors de l'ajout d'un gestionnaire de zone ou d'un utilisateur, cliquez sur une zone pour les attribuer.
6. Cliquez sur **Ajouter**. Un e-mail est envoyé à l'utilisateur. Il contient un lien permettant de créer un mot de passe.

Pour modifier les rôles des utilisateurs

1. Connectez-vous à la console (http://dellthreatdefense.com) en tant qu'administrateur. Seuls les administrateurs peuvent créer des utilisateurs.
2. Sélectionnez **Paramètres > Gestion des utilisateurs**.
3. Cliquez sur un utilisateur. La page Détail de l'utilisateur s'affiche.
4. Sélectionnez un rôle, puis cliquez sur **Enregistrer**.

Pour supprimer des utilisateurs

1. Connectez-vous à la console (http://dellthreatdefense.com) en tant qu'administrateur. Seuls les administrateurs peuvent créer des utilisateurs.
2. Sélectionnez **Paramètres > Gestion des utilisateurs**.
3. Cochez la case du ou des utilisateurs à supprimer.
4. Cliquez sur **Supprimer**.
5. Cliquez sur **Oui** dans le message vous invitant à confirmer la suppression.

Options liées au réseau

Configurez le réseau de manière à autoriser l'agent Threat Defense à communiquer avec la console sur Internet. Cette section présente les paramètres de pare-feu et la configuration du proxy.

Pare-feu

Aucun logiciel sur site n'est nécessaire pour gérer les périphériques. Les agents Threat Defense sont gérés par la console (interface utilisateur basée dans le cloud) et lui font leurs rapports. Le port 443 (HTTPS) est utilisé pour la communication et doit être ouvert sur le pare-feu pour que les agents puissent communiquer avec la console. La console est hébergée par Amazon Web Services (AWS) et ne possède pas d'adresse IP fixe. Vérifiez que les agents peuvent communiquer avec les sites suivants :

- login.cylance.com
- data.cylance.com
- my.cylance.com
- update.cylance.com
- api2.cylance.com
- download.cylance.com

Autre solution : autorisez le trafic HTTPS avec *.cylance.com.

Proxy

Vous configurez la prise en charge du proxy pour Threat Defense via une entrée de registre. Si un proxy est configuré, l'agent utilise l'adresse IP et le port figurant dans l'entrée de registre pour toutes les communications sortantes en direction des serveurs de console.

1. Accédez au registre.

   Remarque : vous devez disposer de privilèges de haut niveau ou être propriétaire du registre, selon la façon dont l'agent a été installé (Mode Protégé activé ou non).

2. Dans l'Éditeur de registre, accédez à la clé **`HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`**.
3. Créez une nouvelle valeur Chaîne (REG_SZ) :
   - Nom de la valeur = ProxyServer
   - Données de la valeur = paramètres de proxy (par exemple, http://123.45.67.89:8080)

L'agent tente d'utiliser les informations d'identification de l'utilisateur actuellement connecté pour les communications sortantes vers Internet dans les environnements authentifiés. Si vous avez configuré un proxy authentifié et qu'aucun utilisateur n'est connecté au périphérique, l'agent ne peut pas s'authentifier auprès du proxy et ne peut pas communiquer avec la console. Solutions à appliquer dans ce cas :

- Configurez le proxy et ajoutez une règle pour autoriser tout le trafic vers *.cylance.com.
- Utilisez une autre stratégie de proxy, qui autorise l'accès proxy sans authentification aux hôtes Cylance (*.cylance.com).

Lorsque vous procédez ainsi, si aucun utilisateur n'est connecté au périphérique, l'agent n'a pas besoin de s'authentifier, et il devrait pouvoir se connecter au cloud et communiquer avec la console.

Périphériques

Une fois l'agent installé sur un point de terminaison, il devient disponible en tant que périphérique dans la console. Commencez par gérer les périphériques en attribuant la stratégie (pour gérer les *menaces* identifiées), puis regroupez les périphériques (à l'aide des *zones*) et intervenez manuellement sur tous les périphériques (en les *mettant en quarantaine* et en les *ignorant*, le cas échéant).

Gestion des périphériques

Le terme « périphérique » désigne les ordinateurs où l'agent Threat Defense est installé. Vous gérez les périphériques depuis la console.

1. Connectez-vous à la console (http://dellthreatdefense.com) en tant qu'administrateur. Seuls les administrateurs peuvent gérer les périphériques.
2. Cliquez sur **Périphériques**.
3. Cochez la case d'un périphérique pour autoriser les actions suivantes :
    - **Exporter** : permet de créer et de télécharger un fichier .CSV. Le fichier contient des informations (Nom, État et Stratégie) sur tous les périphériques de l'entreprise.
    - **Supprimer** : permet de supprimer les périphériques sélectionnés de la *liste des périphériques*. Cela ne désinstalle pas l'agent du périphérique.
    - **Attribuer une stratégie** : permet d'attribuer une stratégie aux périphériques sélectionnés.
    - **Ajouter à des zones** : permet d'ajouter les périphériques sélectionnés à une ou plusieurs zones.
4. Cliquez sur un périphérique pour afficher la page Détails du périphérique.
    - **Informations sur le périphérique** : affiche des informations comme le nom d'hôte, la version de l'agent et la version du système d'exploitation.
    - **Propriétés du périphérique** : permet de modifier le nom du périphérique, la stratégie, les zones et le niveau de journalisation.
    - **Menaces et activités** : affiche les informations concernant les menaces et autres activités liées au périphérique.
5. Cliquez sur **Ajouter un nouveau périphérique** pour afficher une boîte de dialogue contenant le jeton d'installation ainsi que des liens permettant de télécharger le programme d'installation de l'agent.
6. Dans la colonne Zones, cliquez sur un nom de zone pour afficher la page Détails de la zone.

Menaces et activités

Affiche les informations concernant les menaces et autres activités liées au périphérique sélectionné.

Menaces

Affiche toutes les menaces détectées sur le périphérique. Par défaut, les menaces sont regroupées par état (*Dangereux*, *Anormal*, *Mis en quarantaine* et *Ignoré*).

- **Exporter** : permet de créer et de télécharger un fichier CSV contenant des informations sur toutes les menaces détectées sur les périphériques sélectionnés. Les informations de menace incluent le nom, le chemin du fichier, le score Cylance et l'état.

- **Mettre en quarantaine** : permet de *mettre en quarantaine* les menaces sélectionnées. Il s'agit d'une *quarantaine locale*, ce qui signifie que les menaces sélectionnées sont uniquement *mises en quarantaine* sur ce périphérique. Pour *mettre en quarantaine* une menace pour tous les périphériques de l'entreprise, assurez-vous que la case **Mettre également en quarantaine cette menace chaque fois qu'elle est détectée sur un périphérique** est cochée (*Quarantaine globale*) lorsqu'un fichier est *mis en quarantaine*.
- **Ignorer** : définit l'état des menaces sélectionnées sur *Ignoré*. Un fichier *ignoré* peut s'exécuter. Il s'agit d'une *quarantaine locale*, ce qui signifie que le fichier peut uniquement s'exécuter sur ce périphérique. Pour permettre à ce fichier de s'exécuter sur tous les périphériques de l'entreprise, cochez la case **Marquer également comme sûr sur tous les périphériques** (*liste de confiance*) lorsque vous définissez un fichier comme *Ignoré*.

Tentatives d'exploitation

Affiche toutes les tentatives d'exploitation détectées sur le périphérique. Cela comprend des détails comme le nom du processus, son ID, son type et l'action réalisée.

Journaux d'agent

Affiche les fichiers journaux téléchargés par l'agent sur le périphérique. Le nom du fichier journal correspond à sa date de création.

Pour afficher les fichiers journaux d'agent :

1. Téléchargez le fichier journal actuel d'un seul périphérique.
   a. Cliquez sur Périphériques > Journaux d'agent.
   b. Cliquez sur **Télécharger le fichier de journal actuel**. L'opération peut prendre plusieurs minutes, selon la taille du fichier journal.

OU

1. Paramètres de stratégie :
   a. Cliquez sur Paramètres > Règle de périphérique > [sélectionnez une règle] > Journaux d'agent.
   b. Cliquez sur Activer le téléchargement auto des fichiers journaux.
   c. Cliquez sur **Enregistrer**.

Pour afficher des journaux en mode détaillé (verbose), changez le niveau de journalisation de l'agent avant de télécharger les journaux.

1. Dans la console : **Périphériques > [cliquez sur un périphérique]**, sélectionnez le mode **Détaillé (verbose)** dans le menu déroulant Niveau de journalisation de l'agent, puis cliquez sur **Enregistrer**. Une fois les journaux détaillés (verbose) téléchargés, Dell vous recommande de rétablir le niveau de journalisation d'agent *Informations*.
2. Sur le périphérique, fermez l'interface utilisateur Threat Defense (effectuez un clic droit sur l'icône Threat Defense dans la barre d'état système, puis cliquez sur **Quitter**).

OU

1. Accédez à l'interface de ligne de commande en tant qu'administrateur. Saisissez la commande suivante et appuyez sur **Entrée**.

   ```
   cd C:\Program Files\Cylance\Desktop
   ```

2. Saisissez la commande suivante et appuyez sur **Entrée**.

   ```
   Dell.ThreatDefense.exe -a
   ```

3. L'icône Threat Defense s'affiche dans la barre d'état système. Effectuez un clic droit, sélectionnez **Journalisation**, puis cliquez sur **Tout** (identique au niveau détaillé (verbose) dans la console).

OU (Pour macOS)

1. Quittez l'interface utilisateur en cours d'exécution.
2. Accédez à la fenêtre de terminal et exécutez la commande suivante.

   ```
   sudo /Applications/Cylance/CylanceUI.app/Contents/MacOS/CylanceUI -a
   ```

3. Effectuez un clic droit sur la nouvelle interface utilisateur lorsqu'elle s'ouvre. Sélectionnez **Journalisation > Tout**.

Contrôle des scripts

Affiche toutes les activités liées au contrôle des scripts, notamment les scripts interdits.

Périphériques en double

Lors de l'installation initiale de l'agent Threat Defense sur un périphérique, un ID unique est créé. La console l'utilise pour identifier ce périphérique et y faire référence. Cependant, certains événements, comme l'utilisation d'une image de machine virtuelle pour créer plusieurs systèmes, peuvent provoquer la génération d'un second ID pour le même périphérique. Sélectionnez le périphérique, puis cliquez sur **Supprimer** lorsqu'une entrée en double s'affiche sur la page Périphériques de la console.

Pour faciliter l'identification de ce type de périphérique, utilisez la fonction de tri des colonnes de la page Périphériques afin de trier les périphériques et de les comparer, généralement sur la base de leur nom. Vous avez également la possibilité d'exporter la *liste des périphériques* en tant que fichier .CSV et de l'afficher dans Microsoft Excel ou une application similaire dotée de puissantes fonctions de tri et d'organisation.

Exemple avec Microsoft Excel

1. Ouvrez le fichier CSV des périphériques dans Microsoft Excel.
2. Sélectionnez la colonne des noms de périphérique.
3. Dans l'onglet Accueil, sélectionnez Mise en forme conditionnelle > Règles de mise en surbrillance des cellules > Valeurs en double).
4. Vérifiez que **Doublon** est sélectionné, puis sélectionnez une option de mise en surbrillance.
5. Cliquez sur **OK**. Les éléments en double sont mis en surbrillance.

Remarque : la commande Supprimer permet seulement de supprimer le périphérique de la page Périphériques. Elle n'envoie pas de commande de désinstallation à l'agent Threat Defense. L'agent doit être désinstallé sur le point de terminaison.

Mise à jour de l'agent

La maintenance et la gestion des agents Threat Defense sont très simples. Les agents téléchargent automatiquement les mises à jour depuis la console et la maintenance de cette dernière est assurée par Cylance.

L'agent prend contact avec la console toutes les 1-2 minutes. La console indique l'état actuel de l'agent (*En ligne* ou *Hors ligne*, *Dangereux* ou *Protégé*), les informations de version, le système d'exploitation et l'état de la menace.

Threat Defense publie des mises à jour de l'agent tous les mois. Ces mises à jour peuvent comprendre des révisions de la configuration, de nouveaux modules et des modifications du programme. Lorsqu'une mise à jour de l'agent est disponible (la console vous le signale sous Settings > Agent Updates [Paramètres > Mises à jour de l'agent]), l'agent télécharge et applique automatiquement cette mise à jour. Pour contrôler le trafic réseau pendant la mise à jour de l'agent, toutes les entreprises sont configurées pour autoriser un maximum de 1 000 mises à jour de périphérique simultanées. Les utilisateurs peuvent également désactiver la fonction Mise à jour auto s'ils le souhaitent.

Remarque : le support Dell peut modifier le nombre maximal de périphériques pouvant être mis à jour simultanément.

Mise à jour sur la base des zones

La mise à jour sur la base des zones permet à une entreprise de tester un nouvel agent sur un petit nombre de périphériques avant de le déployer dans l'ensemble de son environnement (Production). Vous pouvez ajouter temporairement une ou plusieurs des zones actuelles à l'une des deux zones de test (Test et Pilote) qui vous permettent d'utiliser un agent différent de celui de l'environnement de production.

Pour configurer la mise à jour sur la base des zones :

1. Connectez-vous à la console (http://dellthreatdefense.com) à l'aide d'un compte administrateur.
2. Sélectionnez **Paramètres > Mise à jour de l'agent**. Les trois dernières versions de l'agent s'affichent.

   Si la zone Production est définie sur **Mise à jour auto**, les zones de test et zones pilotes ne sont pas disponibles. Pour activer les zones de test et zones pilotes, remplacez l'option Mise à jour auto de la zone Production par une autre option.
3. Sélectionnez une version spécifique de l'agent dans la liste déroulante Production.
4. Pour Production, sélectionnez également Mise à jour auto ou Ne pas mettre à jour.
   a. L'option **Mise à jour auto** permet à tous les périphériques de production d'être automatiquement mis à jour vers la dernière version de la *liste Versions de l'agent prises en charge*.
   b. L'option **Ne pas mettre à jour** empêche tous les périphériques de production de mettre à jour l'agent.
5. Pour la zone Test, choisissez une ou plusieurs zones dans la liste déroulante Zone, puis choisissez une version spécifique de l'agent dans la liste déroulante des versions.
6. Si nécessaire, répétez l'étape 5 pour la zone Pilote.

Remarque : si vous ajoutez un périphérique à une zone incluse dans la zone Test ou Pilote, ce périphérique commence à utiliser la version d'agent de la zone Test ou Pilote. Si un périphérique appartient à plusieurs zones dont une seule est incluse dans la zone Test ou Pilote, la version d'agent de la zone Test ou Pilote est prioritaire.

Pour déclencher une mise à jour de l'agent

Pour déclencher une mise à jour de l'agent avant que le délai d'une heure en cours soit écoulé :

1. Effectuez un clic droit sur l'icône de l'agent Threat Defense dans la barre d'état système, puis cliquez sur **Rechercher des mises à jour**.
2. Redémarrez le service Threat Defense. Cela le force à prendre immédiatement contact avec la console.

OU

- Vous pouvez lancer les mises à jour à partir de la ligne de commande. Exécutez la commande suivante depuis le répertoire Cylance :

  ```
  Dell.ThreatDefense.exe – update
  ```

Tableau de bord

La page Tableau de bord apparaît une fois que vous êtes connecté à la console Threat Defense. Le tableau de bord fournit une vue d'ensemble des menaces de votre environnement et vous permet d'accéder aux différentes informations de la console sur une seule page.

Statistiques de menace

Les statistiques de menace indiquent le nombre de menaces détectées au cours des *dernières 24 heures* ainsi que le nombre *total* de menaces de l'entreprise. Cliquez sur *Statistiques de menace* pour accéder à la page Protection et afficher la liste des menaces associées à cette statistique.

- **Menaces en cours d'exécution** : fichiers identifiés comme des menaces, actuellement en cours d'exécution sur les périphériques de l'entreprise.
- **Menaces à exécution auto** : menaces configurées pour s'exécuter automatiquement.
- **Menaces mises en quarantaine** : menaces *mises en quarantaine* au cours des 24 heures et total des menaces.
- **Menaces spécifiques à Cylance** : menaces identifiées par Cylance mais pas par d'autres sources d'antivirus.

Pourcentages de protection

Affiche les pourcentages correspondant à la protection contre les menaces et à la protection des périphériques.

- **Protection contre les menaces** : pourcentage de menaces auxquelles une action a été appliquée (Quarantaine, Quarantaine globale, Ignorer et Listes de confiance).
- **Protection des périphériques** : pourcentage de périphériques associés à une stratégie où l'option Quarantaine auto est activée.

Menaces par priorité

Affiche le nombre total des menaces qui nécessitent une action (*Quarantaine*, *Quarantaine globale*, *Ignorer* et *Listes de confiance*). Les menaces sont regroupées par priorité (Élevée, Moyenne ou Faible). Cette vue d'ensemble affiche le nombre total de menaces qui nécessitent une action, divisées par niveau de priorité. Elle affiche également le pourcentage total et indique le nombre de périphériques concernés.

Les menaces sont triées par ordre de priorité dans l'angle inférieur gauche de la page Tableau de bord. L'écran spécifie le nombre total de menaces de l'entreprise, regroupées par niveau de priorité.

Une menace est classée au niveau Faible, Moyen ou Élevé en fonction du nombre des attributs suivants qu'elle présente :

- Le fichier possède un score Cylance supérieur à 80.
- Le fichier est en cours d'exécution.
- Le fichier a été exécuté précédemment.
- Le fichier est configuré pour exécution automatique.
- Priorité de la zone où la menace a été détectée.

Cette classification permet aux administrateurs de déterminer les menaces et périphériques à traiter en premier. Cliquez sur la menace ou sur le nombre de périphériques pour afficher les détails de la menace et des périphériques.

Événements de menace

Affiche un diagramme à lignes montrant le nombre de menaces détectées sur les 30 derniers jours. Les lignes sont codées par couleur pour les fichiers *dangereux*, *anormaux*, *mis en quarantaine*, *ignorés* et *effacés*.

- Placez la souris sur un point du diagramme pour afficher les détails correspondants.
- Cliquez sur l'une des couleurs de la légende pour afficher ou masquer la ligne correspondante.

Classification des menaces

Affiche une carte à zones sensibles des divers types de menace détectés dans l'entreprise (comme les virus ou les programmes malveillants). Cliquez sur un élément dans la carte à zones sensibles pour accéder à la page Protection et afficher la liste des menaces du type concerné.

Listes « 5 principales »

Affiche les listes 5 principales menaces détectées sur le plus grand nombre de périphériques, 5 principaux périphériques avec le plus de menaces et 5 principales zones avec le plus de menaces dans l'entreprise. Cliquez sur une entrée de liste pour obtenir des détails.

Les listes « 5 principales » du tableau de bord mettent en surbrillance les menaces *dangereuses* de l'entreprise qui n'ont encore fait l'objet d'aucune intervention, comme les menaces *mises en quarantaine* ou *ignorées*. La plupart du temps, ces listes devraient être vides. Bien que les menaces *anormales* exigent également d'être traitées, les listes « 5 principales » attirent votre attention sur les menaces critiques.

Protection – Menaces

Threat Defense peut faire bien plus que simplement classer les fichiers comme *dangereux* ou *anormaux*. Cette solution peut fournir des détails sur les caractéristiques statiques et dynamiques des fichiers. Cela permet aux administrateurs non seulement de bloquer les menaces, mais aussi de comprendre le comportement de ces menaces afin de les atténuer ou d'y répondre.

Type de fichier

Dangereux : fichier avec un score entre 60 et 100. Un fichier *dangereux* est un fichier dans lequel le moteur Threat Defense identifie des attributs qui ressemblent fortement à un programme malveillant.

Anormal : fichier avec un score entre 1 et 59. Un fichier anormal a quelques attributs de programme malveillant, mais moins qu'un fichier *dangereux*, et est donc moins susceptible d'être un programme malveillant.

Remarque : il arrive qu'un fichier soit classé comme *dangereux* ou *anormal*, même si le score affiché ne correspond pas à la plage de la classification. Cela peut être dû aux toutes dernières constatations ou à une analyse de fichier supplémentaire réalisée après la détection initiale. Pour consulter l'analyse la plus à jour, activez Téléchargement auto dans la stratégie de périphérique.

Score Cylance

Un score Cylance est attribué à chaque fichier considéré comme *anormal* ou *dangereux*. Le score indique le degré de probabilité qu'il s'agisse d'un fichier de programme malveillant. Plus le chiffre est élevé, plus le degré de probabilité est élevé.

Affichage des informations de menace

L'onglet Protection de la console affiche des informations détaillées sur les menaces, en précisant les périphériques où elles ont été détectées et les actions appliquées à ces périphériques en réaction à ces menaces.

Remarque : vous pouvez configurer les colonnes de la *liste des menaces* de l'onglet Protection. Cliquez sur la flèche vers le bas d'une colonne pour ouvrir le menu associé, puis affichez/masquez les différents détails concernant les menaces. Le menu inclut un sous-menu de filtrage.

Pour afficher les détails de menace

1. Connectez-vous à la console (http://dellthreatdefense.com).
2. Cliquez sur l'onglet **Protection** pour afficher la liste des menaces identifiées dans l'entreprise.
3. Utilisez le filtre de la barre de menus de gauche pour filtrer la liste par priorité (Élevée, Moyenne ou Faible) et par état (*Mis en quarantaine*, *Ignoré*, *Dangereux* ou *Anormal*).

Remarque : les nombres affichés en rouge dans le volet de gauche signalent les menaces en attente qui n'ont pas encore été *mises en quarantaine* ou *ignorées*. Filtrez l'affichage sur la base de ces éléments pour afficher la liste des fichiers qui doivent être examinés.

4. Pour ajouter des colonnes afin de pouvoir afficher des informations supplémentaires sur les menaces, cliquez sur la flèche vers le bas près des noms de colonne et sélectionnez un nom.
5. Pour afficher des informations supplémentaires sur une menace spécifique, cliquez sur le lien de nom de cette menace (les détails s'affichent dans une nouvelle page) ou cliquez n'importe où dans la ligne de la menace (les détails s'affichent au bas de la page). Les deux vues affichent le même contenu mais dans une présentation différente. Les détails disponibles incluent une présentation des métadonnées du fichier, la liste des périphériques où la menace a été détectée et des rapports de preuve.
    a. Métadonnées de fichier
        - Classification [attribuée par l'équipe Advanced Threat and Alert Management (ATAM) de Cylance]
        - Score Cylance (niveau de confiance)
        - Opinion de l'industrie des antivirus (liens vers VirusTotal.com pour comparaison avec d'autres fournisseurs)
        - Date de première détection et date de dernière détection
        - SHA256
        - MD5
        - Informations de fichier (auteur, description, version, etc.)
        - Détails de signature
    b. Périphériques

        La *liste de périphériques/zones* correspondant à une menace peut être filtrée en fonction de l'état de la menace (*Dangereux*, *Mis en quarantaine*, *Ignoré* et *Anormal*). Cliquez sur le lien de filtre d'état pour afficher les périphériques qui présentent la menace dans cet état.
        - *Dangereux* : le fichier est classé comme *dangereux*, mais aucune action n'a été entreprise.
        - *Mis en quarantaine* : le fichier a déjà été *mis en quarantaine* en raison d'un paramètre de stratégie.
        - *Ignoré* : le fichier a été *ignoré* ou *mis en liste blanche* par l'administrateur.
        - *Anormal* : le fichier est classé comme *anormal*, mais aucune action n'a été entreprise.
    c. Rapports de preuve
        - **Indicateurs de menace** : observations concernant un fichier que le moteur Cylance Infinity a analysé. Ces indicateurs vous aident à comprendre la raison de la classification d'un fichier, et fournissent des détails sur les attributs et le comportement de ce fichier. Les indicateurs de menace sont regroupés en catégories pour offrir une aide contextuelle.
        - **Données de menace détaillées** : la section Données de menace détaillées fournit un récapitulatif complet des caractéristiques statiques et dynamiques d'un fichier, notamment des métadonnées de fichier supplémentaires, les détails de la structure du fichier, ainsi que ses comportements dynamiques, comme la suppression de fichiers, la création ou la modification de clés de registre, et les URL avec lesquelles il a tenté de communiquer.

Pour afficher les indicateurs de menace :

1. Connectez-vous à la console (http://dellthreatdefense.com).
2. Cliquez sur **Protection** dans le menu supérieur pour afficher la liste des menaces (ou cliquez sur **Périphériques**, puis sélectionnez un périphérique).
3. Cliquez sur un nom de menace. La page Détails de la menace s'affiche.
4. Cliquez sur **Rapports de preuve**.

Catégories d'indicateurs de menace :

chaque catégorie représente un aspect fréquemment constaté dans les logiciels malveillants, sur la base d'une analyse en profondeur de plus de 100 millions de fichiers binaires. Le rapport Indicateurs de menace indique le nombre de ces catégories détectées dans le fichier.

Anomalies
Le fichier comporte des éléments incohérents ou anormaux. Souvent, il s'agit d'incohérences dans la structure du fichier.

Collecte
Le fichier montre des traces de collecte de données. Il peut s'agir d'une énumération de la configuration de périphérique ou de la collecte d'informations sensibles.

Perte de données
Le fichier montre des traces de données en sortie. Il peut s'agir de connexions réseau sortantes, d'une preuve que le système a servi de navigateur ou d'autres communications réseau.

Tromperie
Le fichier montre des traces d'une tentative de tromperie. La tromperie peut se manifester par des sections masquées, l'inclusion d'un code pour éviter la détection ou de signes d'étiquetage incorrect des métadonnées ou d'autres sections.

Destruction
Le fichier montre des traces de fonctions de destruction. La destruction est notamment la capacité à supprimer des ressources sur un périphérique, comme des fichiers ou des répertoires.

Divers
Tous les indicateurs non classés dans les autres catégories.

Remarque : parfois, les sections Indicateurs de menace et Données de menace détaillées ne comportent aucun résultat ou ne sont pas disponibles. Cela se produit lorsque le fichier n'a pas été téléchargé. Le journal de débogage peut fournir des détails sur la raison pour laquelle le fichier n'a pas été téléchargé.

Traitement des menaces

Le type d'action à appliquer à certaines menaces peut dépendre de l'utilisateur affecté au périphérique. Les actions appliquées aux menaces peuvent l'être au niveau du périphérique ou au niveau global. Voici les différentes actions que vous pouvez appliquer aux menaces ou aux fichiers détectés :

- ***Mettre en quarantaine*** : mettre un fichier *en quarantaine* pour empêcher son exécution sur ce périphérique.

  Remarque : Vous pouvez mettre une menace en quarantaine à l'aide de la ligne de commande sur un périphérique. Cette fonctionnalité est uniquement disponible avec l'agent Windows. Pour plus d'informations, voir Mise en quarantaine par ligne de commande.

- ***Quarantaine globale*** : mettre un fichier *en quarantaine globale* pour l'empêcher de s'exécuter sur tous les périphériques de l'entreprise.

  Remarque : la *mise en quarantaine* d'un fichier le déplace de son emplacement d'origine vers le répertoire de *quarantaine* (`C:\ProgramData\Cylance\Desktop\q`).

- ***Ignorer*** : si vous *ignorez* un fichier spécifique, vous l'autorisez à s'exécuter sur le périphérique.
- ***Confiance globale*** : l'inscription d'un fichier sur une *liste de confiance globale* l'autorise à s'exécuter sur tous les périphériques de l'entreprise.

  Remarque : parfois, Threat Defense peut *mettre en quarantaine* ou signaler un fichier « sain » (surtout si les caractéristiques de ce fichier ressemblent fortement à celles de fichiers malveillants). Dans ce cas, il peut s'avérer utile d'*ignorer* le fichier ou de le *placer dans la liste de confiance globale*.
- ***Charger le fichier*** : permet de télécharger manuellement un fichier vers Cylance Infinity pour analyse. Si vous avez activé le téléchargement automatique, les nouveaux fichiers (pas encore analysés par Cylance) sont automatiquement téléchargés vers Cylance Infinity. Si le fichier existe déjà dans Cylance Infinity, le bouton Télécharger le fichier vers Cylance n'est pas disponible (grisé).
- ***Télécharger le fichier*** : vous permet de télécharger un fichier pour effectuer vos propres tests. Cette fonction doit avoir été activée pour l'entreprise. L'utilisateur doit avoir des droits Administrateur. La menace doit avoir été détectée par un agent de version 1320 ou supérieure.

  Remarque : le fichier doit être disponible dans Cylance Infinity et ses 3 valeurs de hachage (SHA256, SHA1 et MD5) doivent être identiques dans Cylance Infinity et dans l'agent. Sinon, le bouton Télécharger le fichier n'est pas disponible.

Traitement des menaces sur un périphérique spécifique

1. Connectez-vous à la console (http://dellthreatdefense.com) en tant qu'administrateur ou gestionnaire de zone.
2. Cliquez sur l'onglet **Périphériques**.
3. Recherchez et sélectionnez le périphérique voulu.
4. Vous pouvez également utiliser le lien vers le périphérique qui figure dans l'onglet Protection si une menace est signalée sur ce périphérique.
5. Toutes les menaces de ce périphérique sont répertoriées au bas de la page. Sélectionnez la menace pour *mettre en quarantaine* ou *ignorer* le fichier sur ce périphérique.

Traitement des menaces au niveau global

Les fichiers ajoutés à la *liste Quarantaine globale* ou à la *liste de confiance globale* sont soit *mis en quarantaine*, soit *autorisés* sur tous les périphériques de toutes les zones.

1. Connectez-vous à la console (http://dellthreatdefense.com) en tant qu'administrateur.
2. Cliquez sur **Paramètres > Liste globale**.
3. Cliquez sur Quarantaine globale ou sur Liste de confiance globale.
4. Cliquez sur **Ajouter un fichier**.
5. Ajoutez les valeurs de hachage SHA256 (obligatoire) et MD5 du fichier, son nom et la raison pour laquelle vous le placez dans la *Liste globale*.
6. Cliquez sur **Envoyer**.

Protection – Contrôle des scripts

Threat Defense fournit des détails sur les scripts Active Script et PowerShell qui ont été bloqués ou ont déclenché une alerte. Si vous avez activé Contrôle des scripts, les résultats s'affichent dans l'onglet Contrôle des scripts de la page Protection. Vous y trouverez des détails sur le script et sur les périphériques concernés.

Pour afficher les résultats de Contrôle des scripts

1. Connectez-vous à la console (http://dellthreatdefense.com) en tant qu'administrateur.
2. Cliquez sur Protection.
3. Cliquez sur Contrôle des scripts.
4. Sélectionnez un script dans la table. Cela met à jour la table Détails avec la liste des périphériques concernés.

Description des colonnes Contrôle des scripts

- **Nom du fichier** : nom du script.
- **Interpréteur** : fonction de contrôle des scripts qui a identifié le script.
- **Dernière détection** : date et heure de la dernière exécution du script.
- **Type de lecteur** : type du lecteur où le script a été détecté (exemple : Disque dur interne).
- **SHA256** : valeur de hachage SHA256 du script.
- **Nb de périphériques** : nombre de périphériques concernés par ce script.
- **Alerte** : nombre de fois où le script a déclenché une alerte. Il peut y avoir plusieurs occurrences pour le même périphérique.
- **Bloquer** : nombre de fois où le script a été bloqué. Il peut y avoir plusieurs occurrences pour le même périphérique.

Description des colonnes Détails

- **Nom du périphérique** : nom du périphérique affecté par ce script. Cliquez sur le nom du périphérique pour afficher la page Détails du périphérique.
- **Affirmation** : état du périphérique (en ligne ou hors ligne).
- **Version de l'agent** : numéro de la version de l'agent actuellement installée sur le périphérique.
- **Chemin d'accès au fichier** : chemin de fichier depuis lequel le script a été exécuté.
- **Quand** : date et heure d'exécution du script.
- **Nom d'utilisateur** : nom de l'utilisateur connecté au moment où le script a été exécuté.
- **Action** : action à appliquer au script (Alerte ou Bloquer).

Liste globale

Une *liste globale* permet de sélectionner un fichier pour la *mise en quarantaine* ou au contraire d'*autoriser* son exécution sur tous les périphériques de l'entreprise.

- **Quarantaine globale :** tous les agents de l'entreprise *mettent en quarantaine* tout fichier présent dans la *liste Quarantaine globale* détecté sur le périphérique.

- **Liste de confiance globale :** tous les agents de l'entreprise *autorisent* tout fichier présent dans la *liste de confiance globale* détecté sur le périphérique.
- **Non attribué :** désigne toutes les menaces identifiées dans l'entreprise qui ne sont attribués ni à la *liste Quarantaine globale*, ni à la *liste de confiance globale*.

Modification de l'état d'une menace

Permet de modifier l'état d'une menace (*Quarantaine globale*, *Liste de confiance* ou *Non attribué*) :

1. Connectez-vous à la console (http://dellthreatdefense.com) en tant qu'administrateur.
2. Sélectionnez **Paramètres > Liste globale**.
3. Sélectionnez la liste à laquelle la menace est actuellement associée. Par exemple, cliquez sur Non attribué pour définir l'état d'une menace non attribuée sur *Liste de confiance* ou *Quarantaine globale.*
4. Cochez les cases des menaces à modifier, puis cliquez sur un bouton d'état.
    a. Liste de confiance globale : déplace les fichiers dans la *liste de confiance*.
    b. Quarantaine globale : déplace les fichiers dans la *liste Quarantaine globale*.
    c. Supprimer de la liste : déplace les fichiers dans la *liste Non attribué.*

Ajout d'un fichier

Ajoutez manuellement un fichier à la *liste Quarantaine globale* ou à la *liste de confiance globale*. La valeur de hachage SHA256 du fichier que vous ajoutez est obligatoire.

1. Connectez-vous à la console (http://dellthreatdefense.com) en tant qu'administrateur.
2. Sélectionnez **Paramètres > Liste globale**.
3. Sélectionnez la liste dans laquelle placer le fichier (*Quarantaine globale* ou *Liste de confiance globale*).
4. Cliquez sur **Ajouter un fichier**.
5. Entrez la valeur de hachage SHA256. (Facultatif) Indiquez la valeur MD5 et le nom du fichier.
6. Indiquez la raison pour laquelle vous ajoutez ce fichier.
7. Cliquez sur **Envoyer**.

Liste de confiance par certificat

Les clients peuvent placer les fichiers dans la *liste de confiance* en fonction de leur certificat signé, ce qui permet aux logiciels personnalisés dûment signés de s'exécuter sans interruption.

Remarque : actuellement, cette fonction n'est disponible que pour les systèmes d'exploitation Windows.

- Cette fonctionnalité permet aux clients d'établir une *liste blanche*/*liste de confiance* en fonction du certificat signé, représenté par son empreinte SHA1.
- Les informations de certificat sont extraites par la console (Horodatage, Sujet, Émetteur et Empreinte). Le certificat n'est pas téléchargé ni enregistré dans la console.
- L'horodatage du certificat indique la date de création de ce certificat.
- La console ne vérifie pas si le certificat est actif ou s'il a expiré.
- Si le certificat change (s'il est remplacé par un autre ou renouvelé, par exemple), vous devez l'ajouter à la *liste de confiance* de la console.

1. Ajoutez les détails du certificat à la logithèque de certificats.
    a. Identifiez l'empreinte du certificat pour le fichier Portable Executable (PE) signé.
    b. Sélectionnez **Paramètres > Certificats**.
    c. Cliquez sur **Ajouter un certificat**.
    d. Cliquez sur **Rechercher des certificats à ajouter** ou déposez le certificat correspondant dans la zone de message à l'aide de la fonction glisser-déplacer.
    e. Si vous décidez de rechercher manuellement des certificats, la fenêtre Ouvrir s'affiche pour vous permettre de choisir les certificats voulus.
    f. (Facultatif) Ajoutez des remarques sur ce certificat.
    g. Cliquez sur **Envoyer**. Le nom de l'émetteur, le sujet, l'empreinte et les notes (si vous en avez entré) du certificat sont ajoutés à la logithèque.
2. Ajoutez un fichier à la *liste de confiance*.
    a. Sélectionnez **Paramètres > Liste globale**.
    b. Sélectionnez l'onglet **Liste de confiance globale**.
    c. Cliquez sur **Certificats**.
    d. Cliquez sur **Ajouter un certificat**.
    e. Supprimez un certificat de la *liste de confiance*. (Facultatif) Sélectionnez une catégorie et indiquez la raison pour laquelle vous ajoutez ce certificat.
    f. Cliquez sur **Envoyer**.

Affichage des empreintes d'une menace

Dans l'onglet Protection, la section Détails de la menace affiche désormais l'empreinte du certificat. Depuis l'écran, sélectionnez **Ajouter au certificat** pour ajouter le certificat à la logithèque.

Privilèges

Ajouter au certificat est une fonction à laquelle seuls les administrateurs peuvent accéder. Si le certificat a déjà été ajouté à la logithèque de certificats, la console affiche l'option **Accéder au certificat**. Les certificats sont en lecture seule pour les gestionnaires de zone, qui voient l'option **Accéder au certificat**.

Profil

Le menu Profil (angle supérieur droit) vous permet de gérer votre compte, de consulter les journaux d'audit de la console et d'accéder à l'aide du produit.

Mon compte

Modifiez votre mot de passe et vos paramètres de notification par e-mail dans la page Mon compte.

1. Connectez-vous à la console (http://dellthreatdefense.com).
2. Cliquez sur le menu Profil dans l'angle supérieur droit, puis sélectionnez **Mon compte**.
3. Pour modifier votre mot de passe :
    a. Cliquez sur Modifier le mot de passe.
    b. Entrez votre ancien mot de passe.

c. Entrez votre nouveau mot de passe, puis saisissez-le à nouveau pour le confirmer.

d. Cliquez sur Mettre à jour.

4. Cochez ou décochez la case appropriée pour activer/désactiver les notifications par e-mail. L'activation ou la désactivation de l'option est automatiquement enregistrée. Les notifications par e-mail sont disponibles uniquement pour les administrateurs.

Journaux d'audit

Liste déroulante de l'icône d'utilisateur (angle supérieur droit de la console)

Le journal d'audit contient des informations sur les actions suivantes, réalisées depuis la console :

- Connexion (Succès, Échec)
- Stratégie (Ajouter, Modifier, Supprimer).
- Périphérique (Modifier, Supprimer).
- Menace (Quarantaine, Ignorer, Quarantaine globale, Liste de confiance)
- Utilisateur (Ajouter, Modifier, Supprimer).
- Mise à jour de l'agent (Modifier)

Vous pouvez consulter le journal d'audit depuis la console en accédant à la liste déroulante du profil dans l'angle supérieur droit de la console, puis en cliquant sur **Journal d'audit**. Les journaux d'audit sont disponibles uniquement pour les administrateurs.

Paramètres

La page Paramètres comprend les onglets Application, Gestion des utilisateurs, Stratégie de périphérique, Liste globale et Mise à jour de l'agent. L'entrée de menu Paramètres est disponible uniquement pour les administrateurs.

APPLICATION

Agent Threat Defense

Vous ajoutez des périphériques à l'entreprise en installant l'agent Threat Defense sur chaque point de terminaison. Une fois connecté à la console, appliquez une stratégie (pour gérer les menaces identifiées) et organisez vos périphériques en fonction des besoins de l'entreprise.

L'agent Threat Defense est conçu pour utiliser un minimum de ressources système. L'agent traite en priorité les fichiers ou les processus qui s'exécutent, car ils peuvent s'avérer malveillants. Les fichiers simplement stockés sur le disque (mais pas en cours d'exécution) correspondent à niveau de priorité plus faible. En effet, même s'ils peuvent être malveillants, ils ne représentent pas une menace immédiate.

Agent Windows

Configuration système requise

Dell vous recommande de choisir pour vos points de terminaison un matériel (UC, GPU, etc.) qui respecte ou surpasse les recommandations de configuration pour le système d'exploitation concerné. Les exceptions sont signalées ci-après (mémoire RAM, espace disque dur disponible et logiciels supplémentaires requis).

Systèmes d'exploitation	• Windows 7 *(32 et 64 bits)* • Windows Embedded Standard 7 *(32 bits)* et Windows Embedded Standard 7 Pro *(64 bits)* • Windows 8 et 8.1 *(32 et 64 bits)** • Windows 10 (*32 et 64 bits*)** • Windows Server 2008 et 2008 R2 *(32 et 64 bits)**** • Windows Server 2012 et 2012 R2 *(64 bits)**** • Windows Server 2016 – Éditions Standard, Data Center et Essentials*****
RAM	• 2 Go
Espace disque dur disponible	• 300 Mo
Autres logiciels/éléments requis	• .NET Framework 3.5 (SP1) ou supérieur (*Windows uniquement*) • Navigateur Internet • Accès Internet pour la connexion, l'accès au programme d'installation et l'inscription du produit • Droits Administrateur local pour installer le logiciel
Autres conditions requises	• TLS 1.2 est pris en charge avec la version 1422 ou une version supérieure de l'agent et nécessite .NET Framework 4.5 ou une version supérieure

Tableau 2 : Configuration système requise pour Windows

*Non pris en charge : Windows 8,1 RT
**La mise à jour anniversaire Microsoft Windows 10 nécessite la version 1402 ou une version ultérieure de l'agent.
***Non pris en charge : Server Core (2008 et 2012) et Minimal Server (2012).
****Nécessite la version 1412 ou une version ultérieure de l'agent.

Pour télécharger le fichier d'installation

1. Connectez-vous à la console (http://dellthreatdefense.com).
2. Sélectionnez **Paramètres > Application**.
3. Copiez le **jeton d'installation**.

   Le jeton d'installation est une chaîne aléatoire de caractères, générée par le système, qui permet à l'agent de transmettre des données au compte qui lui est attribué dans la console. Le jeton d'installation est obligatoire pour l'installation, que ce soit dans l'Assistant d'installation ou en tant que paramètre d'installation.
4. Téléchargez le programme d'installation.
   a. Sélectionnez le système d'exploitation voulu.
   b. Sélectionnez le type de fichier à télécharger.

      Pour Windows, Dell vous recommande d'utiliser le fichier MSI pour installer l'agent.

Conseil : si vous avez configuré une règle de zone, les périphériques peuvent être automatiquement associés à une zone s'ils répondent aux critères de la règle de zone.

Installation de l'agent – Windows

Vérifiez que tous les prérequis sont respectés avant d'installer Threat Defense. Voir Configuration système requise.

1. Double-cliquez sur DellThreatDefenseSetup.exe (ou le fichier MSI) pour démarrer l'installation.
2. Cliquez sur **Installer** dans la fenêtre de configuration de Threat Defense.
3. Saisissez le jeton d'installation fourni par le locataire Threat Defense. Cliquez sur **Suivant**.

   Remarque : contactez votre administrateur Threat Defense ou consultez l'article de base de connaissances « How To: Manage Threat Defense » (Procédure : Gérer Threat Defense) si l'accès au jeton d'installation est impossible.
4. (Facultatif) Modifiez le dossier de destination de Threat Defense.

   Cliquez sur **OK** pour démarrer l'installation.
5. Cliquez sur **Terminer** pour terminer l'installation. Cochez la case appropriée pour lancer Threat Defense.

Paramètres d'installation Windows

Vous pouvez installer l'agent en mode interactif ou non interactif via GPO, Microsoft System Center Configuration Manager (généralement appelé SCCM) et MSIEXEC. Les fichiers MSI peuvent être personnalisés à l'aide de paramètres intégrés (voir ci-dessous) ou vous pouvez entrer les paramètres sur la ligne de commande.

Propriété	Valeur	Description
PIDKEY	<Jeton d'installation>	Saisie automatique du jeton d'installation
LAUNCHAPP	0 ou 1	0 : l'icône dans la barre d'état système et le dossier du menu Démarrer sont masqués lors de l'exécution. 1 : l'icône dans la barre d'état système et le dossier du menu Démarrer sont visibles lors de l'exécution (valeur par défaut).
SELFPROTECTIONLEVEL	1 ou 2	1 : seuls les administrateurs locaux peuvent modifier le registre et les services. 2 : seul l'administrateur système peut modifier le registre et les services (valeur par défaut).
APPFOLDER	<Dossier d'installation cible>	Indique le répertoire d'installation de l'agent. L'emplacement par défaut est C:\Program Files\Cylance\Desktop.
VenueZone	« Nom_zone »	Nécessite la version 1382 ou une version ultérieure de l'agent •Ajoute des périphériques à une zone. •Si elle n'existe pas, la zone est créée à partir du nom indiqué. •Remplacez nom_zone par le nom d'une zone existante ou de la zone que vous souhaitez créer. **Avertissement** : si vous ajoutez des espaces avant ou après le nom de la zone, une nouvelle zone est créée.

Tableau 3 : Paramètres d'installation pour Windows

L'exemple de ligne de commande suivant montre comment exécuter l'outil Microsoft Windows Installer Tool (MSIEXEC) en lui transmettant les paramètres d'installation PIDKEY, APPFOLDER et LAUNCHAPP :

```
msiexec /i DellThreatDefenseSetup_x64.msi /qn PIDKEY=<JETON D'INSTALLATION>
LAUNCHAPP=0 /L*v C:\temp\install.log
```

L'installation est réalisée en mode silencieux et le journal d'installation est enregistré sous **C:\temp**. Pendant l'exécution de l'agent, l'icône dans la barre d'état système et le dossier Threat Defense du menu Démarrer sont masqués. Vous trouverez des informations supplémentaires sur les commutateurs de ligne de commande acceptés par MSIEXEC dans l'article de base de connaissance KB 227091.

Installation de l'agent Windows avec Wyse Device Manager (WDM)

Cette section explique comment créer un script d'installation, comment créer un paquet RSP pour WDM et comment ajouter le paquet à WDM pour effectuer l'installation sur plusieurs clients légers (Thin Client) simultanément, sans intervention de l'utilisateur.

Créez un script en fichier batch qui exécute l'installation de Threat Defense via la ligne de commande. WDM exécute ce script lors du déploiement.

1. Ouvrez le Bloc-notes. À l'aide des paramètres de ligne de commande ci-dessus, entrez la commande suivante pour exécuter l'installation, en remplaçant **<JETON D'INSTALLATION>** par le jeton qui vous a été fourni : ***msiexec /i C:\TDx86\DellThreatDefense_x86.msi PIDKEY=<JETON D'INSTALLATION> /q***

   C:\TDx86 est utilisé en tant que répertoire, car c'est dans celui-ci que le dossier est copié sur le client léger (Thin Client).

2. Enregistrez le fichier avec l'extension **.bat** dans le dossier TDx86. Par exemple, **TDx86_Install.bat**.

   Créez un paquet RSP permettant l'installation simultanée de l'application Agent Threat Defense sur plusieurs clients légers (Thin Clients) sans intervention de l'utilisateur.

3. Ouvrez Scriptbuilder sur un ordinateur où WDM est installé.

4. Entrez le nom et la description du paquet.

   - Sélectionnez la catégorie de paquets Autres paquets.
   - Sélectionnez le système d'exploitation Windows Embedded Standard 7.

5. Ajoutez des commandes de script pour vérifier si les systèmes cible sont de type WES7 ou WES7p.

   - Sélectionnez Confirm Operating System (CO) (Confirmer le système d'exploitation) sous Commande de script.
   - Sous Device OS (Système d'exploitation du périphérique), indiquez le système d'exploitation approprié.

6. Utilisez les flèches doubles pour ajouter un élément.

7. Appuyez sur **OK** dans l'invite.

8. Ajoutez une commande pour verrouiller le client léger (Thin Client) et interdire toute interaction de l'utilisateur.

   - Sélectionnez **Commande de script > Lockout User (LU)** (Verrouillage utilisateur). Aucune valeur n'est nécessaire. Cependant, dans cet exemple, une **valeur Yes** est entrée, de sorte que l'écran de démarrage soit supprimé si le programme d'installation échoue ou en présence d'une erreur.

9. Ajoutez une commande pour copier les fichiers vers le client léger.
    - Sélectionnez la commande de script **X Copy (XC**) (Copie X).
    - Pour la valeur **Repository Directory** (Répertoire de la logithèque), ajoutez ***** à la fin de la valeur **`<regroot>\`** existante.
    - Pour la valeur **Repository Directory** (Répertoire du périphérique), entrez le chemin d'accès aux fichiers à copier dans les clients légers (Thin Clients) de destination. Dans notre exemple, le nom du paquet est utilisé.
10. Ajoutez une commande pour exécuter le script d'installation .bat.
    - Sélectionnez **Commande de script > Execute on Device (EX)** (Exécuter sur le périphérique).
    - Pour la valeur Device Filename (Nom de fichier du périphérique), entrez le chemin **`C:\TDx86\TDx86_install.bat`**. Le dossier TDx86 est copié par la commande précédente (XC).
    - Ajoutez le signe **+** en tant que valeur Synchronous Execute (Exécution synchrone). Cette option demande à WDM d'attendre la fin de l'exécution du fichier en cours avant de continuer.
11. Ajoutez une commande pour supprimer les fichiers copiés depuis le client léger (Thin Client).
    - Ajoutez la commande de script **Delete Tree (DT)** (Supprimer l'arborescence).
12. Ajoutez des commandes pour désactiver le verrouillage.
    - Ajoutez la commande de script **End Lockout (EL**) (Fin du verrouillage).
13. Lorsque vous le passez en revue, le paquet de script doit ressembler à ce qui suit.
    - Si vous déployez Threat Defense sur des systèmes WES7P, mettez à jour la section relative au système d'exploitation vers WES7P. Sinon, l'installation du paquet échoue.
14. Enregistrez le paquet.
    - Cliquez sur **Enregistrer** et accédez à l'emplacement du dossier **TDx86**, qui devrait se trouver sur le Bureau (si ces instructions ont été respectées).
15. Fermez Scriptbuilder.
16. Lancez **WyseDeviceManager** pour ajouter le paquet à WDM.
17. Accédez à **WyseDeviceManager > Gestionnaire de paquets > Autres paquets**.
18. Sélectionnez **Action > Nouveau > Paquet** dans la barre de menus.
19. Sélectionnez **Enregistrer un paquet à partir d'un fichier de script (.RSP)**, puis cliquez sur **Suivant**.
20. Accédez à l'emplacement du fichier RSP créé à l'étape précédente et cliquez sur **Suivant**.
21. Assurez-vous que la case **Actif** est cochée, puis cliquez sur **Suivant.**
22. Cliquez sur **Suivant** quand WDM est prêt à enregistrer le paquet.
23. Cliquez sur **Terminer** une fois que le paquet a bien été enregistré.
24. Le paquet devient visible sous **Autres paquets**.

25. Vérifiez le contenu du paquet :
    - Ouvrez l'Explorateur de fichiers, accédez à **C:\inetpub\ftproot\Rapport** et localisez le **dossier TDx86**.
    - Ouvrez le dossier TDx86, et vérifiez qu'il contient bien le programme d'installation et le fichier .bat.

Le paquet est désormais disponible dans WDM pour déployer Threat Defense sur plusieurs clients légers (Thin Client) WES7 sans interaction de l'utilisateur.

Mise en quarantaine à l'aide de la ligne de commande

Vous pouvez mettre un fichier en quarantaine à l'aide de la ligne de commande sur un périphérique. Cela nécessite de connaître le code de hachage SHA256 pour la menace.

Remarque : Cette fonctionnalité s'applique uniquement à Windows et nécessite la version 1432 ou une version supérieure de l'agent.

1. Sur le périphérique Windows, ouvrez la ligne de commande. Exemple : Dans le menu Démarrer, recherchez cmd.exe.
2. Lancez Dell.ThreatDefense.exe et incluez l'argument **-q: <hash>**, où <hash> est le code de hachage SHA256 pour le fichier. Cela invitera l'agent à envoyer le fichier vers le dossier de quarantaine.

   Exemple de ligne de commande (Dell Threat Defense installé à l'emplacement par défaut) :

   ```
   "C:\Program Files\Cylance\Desktop\Dell.ThreatDefense.exe" -q:
   14233d4875e148c370a6bbe40fccabccdbfa194dac9e8bd41b0eadcf2351f941
   ```

Désinstallation de l'agent

Pour désinstaller l'agent sur un système Windows, utilisez la ligne de commande ou la fonction Ajout/Suppression de programmes.

La désinstallation de l'agent ne supprime pas l'appareil du Panneau de configuration. Vous devez supprimer manuellement l'appareil du Panneau de configuration.

Avant d'essayer de désinstaller l'agent :

- Si l'option **Exiger un mot de passe pour la désinstallation de l'agent** est activée, vérifiez que vous disposez bien du mot de passe pour le désinstaller.
- Si l'option **Empêcher l'arrêt du service de l'appareil** est activée, désactivez-la dans la stratégie ou appliquez une stratégie différente aux appareils sur lesquels vous souhaitez désinstaller l'agent.

Désinstaller à l'aide de la fonction Ajout/Suppression de programmes

1. Sélectionnez **Démarrer > Panneau de configuration**.
2. Cliquez sur **Désinstaller un programme**. Si des icônes sont sélectionnées à la place des catégories, cliquez sur Programmes et fonctionnalités.
3. Sélectionnez **Dell Threat Defense**, puis cliquez sur **Désinstaller**.

À l'aide de la ligne de commande

1. Accédez à l'invite de commande en tant qu'administrateur.
2. Utilisez les commandes suivantes selon le progiciel d'installation que vous avez utilisé pour installer l'agent.
    a. DellThreatDefense_x64.msi
        i. Désinstallation standard : msiexec /uninstall DellThreatDefense_x64.msi
        ii. Windows Installer : msiexec /x DellThreatDefense_x64.msi
    b. DellThreatDefense_x86.msi
        i. Désinstallation standard : msiexec /uninstall DellThreatDefense_x86.msi
        ii. Windows Installer : msiexec /x DellThreatDefense_x86.msi
3. Les commandes suivantes sont optionnelles :
    a. Pour une désinstallation silencieuse : /quiet
    b. Pour une désinstallation silencieuse et masquée : /qn
    c. Pour une désinstallation de la protection par mot de passe UNINSTALLKEY=<password>
    d. Pour désinstaller le fichier journal : /Lxv* <path>
        i. Cela crée un fichier journal au chemin désigné (<path>), incluant le nom du fichier.
        ii. Exemple : C:\Temp\Uninstall.log

Agent macOS

Configuration système requise

Dell vous recommande de choisir pour vos points de terminaison un matériel (UC, GPU, etc.) qui respecte ou surpasse les recommandations de configuration pour le système d'exploitation concerné. Les exceptions sont signalées ci-après (mémoire RAM, espace disque dur disponible et logiciels supplémentaires requis).

Systèmes d'exploitation	• Mac OS X 10.9 • Mac OS X 10.10 • Mac OS X 10.11 • macOS 10.12* • macOS 10.13**
RAM	• 2 Go
Espace disque dur disponible	• 300 Mo

Tableau 4 : Configuration système requise pour macOS

*Nécessite la version 1412 ou une version ultérieure de l'agent.
** Nécessite la version 1452 ou une version ultérieure de l'agent.

Pour télécharger le fichier d'installation

1. Connectez-vous à la console (http://dellthreatdefense.com).
2. Sélectionnez **Paramètres > Application**.
3. Copiez le **jeton d'installation**.

   Le jeton d'installation est une chaîne aléatoire de caractères, générée par le système, qui permet à l'agent de transmettre des données au compte qui lui est attribué dans la console. Le jeton d'installation est obligatoire pour l'installation, que ce soit dans l'Assistant d'installation ou en tant que paramètre d'installation.
4. Téléchargez le programme d'installation.
   a. Sélectionnez le système d'exploitation voulu.
   b. Sélectionnez le type de fichier à télécharger.

Conseil : si vous avez configuré une règle de zone, les périphériques peuvent être automatiquement associés à une zone s'ils répondent aux critères de la règle de zone.

Installation de l'agent - macOS

Vérifiez que tous les prérequis sont respectés avant d'installer Threat Defense. Voir Configuration système requise.

Remarque : l'agent macOS portera la marque Dell dans les futures versions.

1. Double-cliquez sur **`DellThreatDefense.dmg`** pour monter le programme d'installation.
2. Double-cliquez sur l'icône *Protection* de l'interface utilisateur PROTECT pour démarrer l'installation.
3. Cliquez sur **Continuer** pour vérifier que le système d'exploitation et le matériel sont conformes à la configuration requise.
4. Cliquez sur **Suivant** dans l'écran Introduction.
5. Saisissez le jeton d'installation fourni par le locataire Threat Defense. Cliquez sur **Continuer**.

Remarque : contactez votre administrateur Threat Defense ou consultez l'article de base de connaissances « How To: Manage Threat Defense » (Procédure : Gérer Threat Defense) si l'accès au jeton d'installation est impossible.

6. (Facultatif) Modifiez l'emplacement d'installation de Threat Defense.

   Cliquez sur **Installer** pour démarrer l'installation.
7. Entrez le nom d'utilisateur et le mot de passe d'un administrateur. Cliquez sur **Installer le logiciel**.
8. Cliquez sur **Fermer** dans l'écran Résumé.

Paramètres d'installation macOS

Vous pouvez installer l'agent Threat Defense à l'aide d'options de ligne de commande dans la fenêtre de terminal. Les exemples suivants utilisent le programme d'installation PKG. Pour DMG, modifiez simplement l'extension de fichier dans la commande.

Remarque : vérifiez que les points de terminaison cible respectent la configuration système requise et que la personne qui installe le logiciel dispose des références d'identification correctes pour effectuer cette installation.

Propriété	Valeur	Description
InstallToken		Jeton d'installation disponible dans la console
NoCylanceUI		Masque l'icône de l'agent au démarrage. Valeur par défaut : Visible
SelfProtectionLevel	0 ou 1	1 : seuls les administrateurs locaux peuvent modifier le registre et les services. 2 : seul l'administrateur système peut modifier le registre et les services (valeur par défaut).
LogLevel	0, 1, 2 ou 3	0 : erreur – Seuls les messages d'erreur sont consignés dans les journaux. 1 : avertissement – Les messages d'erreur et d'avertissement sont consignés dans les journaux. 2 : information (valeur par défaut) – Les messages d'erreur, d'avertissement et d'information sont consignés dans les journaux. Cette option peut fournir des détails utiles pour le dépannage. 3 : détaillé (verbose) – Tous les messages sont consignés. Il s'agit du niveau de journalisation recommandé pour le dépannage. Cependant, les fichiers journaux détaillés peuvent devenir très volumineux. Dell vous recommande d'activer le mode Détaillé pour le dépannage, puis de rétablir le mode Information une fois le dépannage terminé.
VenueZone	« Nom_zone »	Nécessite la version 1382 ou une version ultérieure de l'agent •Ajoute des périphériques à une zone. •Si elle n'existe pas, la zone est créée à partir du nom indiqué. •Remplacez nom_zone par le nom d'une zone existante ou de la zone que vous souhaitez créer. **Avertissement** : si vous ajoutez des espaces avant ou après le nom de la zone, une nouvelle zone est créée.

Tableau 5 : Paramètres d'installation pour macOS

Installation de l'agent

Installation sans jeton d'installation

```
sudo installer -pkg DellThreatDefense.pkg -target/
```

Installation avec le jeton d'installation

```
echo [jeton_installation] > cyagent_install_token
sudo installer -pkg DellThreatDefense.pkg -target/
```

Remarque : remplacez **`[jeton_installation]`** par le jeton d'installation. La commande d'écho génère un fichier **`cyagent_install_token`**, qui est un fichier texte contenant une option d'installation par ligne. Ce fichier doit se trouver dans le même dossier que le paquet d'installation. Faites preuve de prudence au niveau des extensions de fichiers : dans l'exemple ci-dessus, le fichier cyagent_install_token ne comprend aucune extension de fichier. Les paramètres par défaut de macOS définissent les extensions comme masquées. La compilation manuelle de ce fichier par édition de texte ou dans un autre éditeur de texte peut ajouter automatiquement une extension qui devra être supprimée.

Paramètres d'installation facultatifs

Saisissez les commandes suivantes dans un terminal pour créer un fichier (**cyagent_install_token**) utilisé par le programme d'installation pour appliquer les options entrées. Chaque paramètre doit se trouver sur sa propre ligne. Ce fichier doit se trouver dans le même dossier que le paquet d'installation.

En voici un exemple. Certains paramètres ne sont pas nécessaires dans ce fichier. La fenêtre Terminal inclut tout ce qui figure entre apostrophes dans le fichier. Veillez à appuyer sur Entrée/Retour après chaque paramètre pour garantir que le fichier contient un seul paramètre par ligne.

Vous pouvez également utiliser un éditeur de texte pour créer ce fichier, en plaçant chaque paramètre sur sa propre ligne. Ce fichier doit se trouver dans le même dossier que le paquet d'installation.

Exemple :

```
echo 'InstallToken

NoCylanceUI

SelfProtectionLevel=2

LogLevel=2'> cyagent_install_token

sudo installer –pkg DellThreatDefense.pkg –target/
```

Désinstallation de l'agent

Sans mot de passe

```
sudo /Applications/Cylance/Uninstall\
DellThreatDefense.app/Contents/MacOS/Uninstall\ DellThreatDefense
```

Avec un mot de passe

```
sudo /Applications/Cylance/Uninstall\
DellThreatDefense.app/Contents/MacOS/Uninstall\ DellThreatDefense --
password=thisismypassword
```

Remarque : remplacez **thisismypassword** par le mot de passe de désinstallation créé dans la console.

Service d'agent

Démarrage du service

```
sudo launchctl load
/Library/launchdaemons/com.cylance.agent_service.plist
```

Arrêt du service

```
sudo launchctl unload
/Library/launchdaemons/com.cylance.agent_service.plist
```

Vérification de l'installation

Contrôlez les points suivants pour vérifier que l'installation de l'agent a réussi.

1. Le dossier de programme a été créé.
    - Valeur par défaut Windows : **`C:\Program Files\Cylance\Desktop`**
    - Valeur par défaut macOS : **`/Applications/DellThreatDefense/`**
2. L'icône Threat Defense est visible dans la barre d'état système du périphérique cible.

    Cela ne s'applique pas si vous avez utilisé les paramètres LAUNCHAPP=0 (Windows) ou NoCylanceUI (macOS).
3. Il existe un dossier Threat Defense sous Menu Démarrer\Tous les programmes sur le périphérique cible.

    Cela ne s'applique pas si vous avez utilisé les paramètres LAUNCHAPP=0 (Windows) ou NoCylanceUI (macOS).
4. Le service Threat Defense a été ajouté et est en cours d'exécution. Le service Threat Defense doit être répertorié comme étant en cours d'exécution dans le volet Services Windows du périphérique cible.
5. Le processus Dell.ThreatDefense.exe est en cours d'exécution. Le processus Dell.ThreatDefense.exe doit apparaître dans l'onglet Processus du Gestionnaire de tâches Windows sur le périphérique cible.
6. Le périphérique communique avec la console. Connectez-vous à la console et cliquez sur l'onglet Périphériques. Le périphérique cible doit être visible et apparaître avec l'état En ligne.

Interface utilisateur de l'agent

L'interface utilisateur de l'agent est activée par défaut. Cliquez sur l'icône de l'agent dans la barre d'état système pour l'afficher. Vous pouvez également installer l'agent de manière à masquer son icône dans la barre d'état système.

Onglet Menaces

Affiche toutes les menaces détectées sur le périphérique, ainsi que l'action appliquée. L'état *Dangereux* indique qu'aucune mesure n'a été prise pour la menace. L'état *Quarantaine* indique que la menace a été modifiée (de façon à empêcher le fichier correspondant de s'exécuter) et a été placée dans le dossier de *quarantaine*. L'état *Ignoré* indique que l'administrateur a estimé que ce fichier était fiable et l'a *autorisé* à s'exécuter sur le périphérique.

Onglet Événements

Affiche tous les événements de menace qui se sont produits sur le périphérique.

Onglet Scripts

Affiche tous les scripts malveillants qui se sont exécutés sur le périphérique, ainsi que l'action appliquée à chaque script.

Menu Agent

Le menu Agent permet d'accéder à l'aide et aux mises à jour de Threat Defense. Il permet également d'accéder à l'interface utilisateur avancée, qui offre davantage d'options de menu.

Menu Agent

Le menu Agent permet aux utilisateurs d'appliquer des actions sur le périphérique. Effectuez un clic droit sur l'icône de l'agent pour afficher le menu.

- **Rechercher des mises à jour** : l'agent recherche les mises à jour disponibles et les installe. Les seules mises à jour autorisées sont celles qui correspondent à la version de l'agent autorisée pour la zone dont le périphérique est membre.

- **Vérifier la mise à jour de règle** : L'agent vérifie si une mise à jour de règle est disponible. Elle peut se définir par des modifications apportées à la règle existante ou une autre règle en cours d'application sur l'agent.

  Remarque : Vérifiez que la mise à jour de règle est prise en charge dans la version 1422 (ou supérieure) pour Windows et la version 1432 (ou supérieure) pour macOS.

- **À propos** : affiche une boîte de dialogue qui contient la version de l'agent, le nom de la stratégie affectée au périphérique, l'heure de dernière recherche de mises à jour par l'agent et le jeton d'installation utilisé pour installer le logiciel.

- **Quitter** : ferme l'icône de l'agent dans la barre d'état système. Cela n'arrête aucun des services Threat Defense.

- **Options > Afficher les notifications** : sélectionnez cette option pour afficher des notifications pour tous les nouveaux événements.

Activation des options avancées de l'interface utilisateur de l'agent

L'agent Threat Defense offre des options avancées, disponibles via l'interface utilisateur, qui permettent d'utiliser des fonctions sur les périphériques sans connexion à la console. Le programme CylanceSVC.exe doit être en cours d'exécution si vous activez les options avancées.

Windows

1. Si l'icône de l'agent est visible dans la barre d'état système, cliquez dessus avec le bouton droit de la souris et sélectionnez **Quitter**.
2. Lancez l'invite de commande et entrez la commande suivante. Appuyez sur Entrée lorsque vous avez terminé.

   ```
   cd C:\Program Files\Cylance\desktop
   ```

   Si l'application a été installée à un autre emplacement, naviguez jusqu'à cet emplacement à l'invite de commande.
3. Entrez la commande suivante et appuyez sur Entrée lorsque vous avez terminé.

   ```
   Dell.ThreatDefense.exe –a
   ```

   L'icône de l'agent apparaît dans la barre d'état système.
4. Effectuez un clic droit sur cette icône. Les options *Journalisation*, *Exécuter une détection* et *Threat Management* s'affichent.

macOS

1. Si l'icône de l'agent est visible dans le menu supérieur, cliquez dessus avec le bouton droit de la souris et sélectionnez **Quitter**.
2. Ouvrez le terminal et exécutez la commande

   a. Sudo /Applications/DellThreatDefense/DellThreatDefense.app/Contents/MacOS/DellThreatDefenseUI –a

   Remarque : il s'agit du chemin d'installation par défaut de Dell Threat Defense. Vous devrez peut-être modifier ce chemin pour l'adapter à votre environnement.
3. L'interface utilisateur de l'agent s'affichera désormais dans les options supplémentaires.

Journalisation
Sélectionnez le niveau d'informations de journal à collecter auprès de l'agent. Valeur par défaut : Information Dell vous recommande de configurer le niveau de journalisation sur Tout (Détaillé) pour le dépannage. Une fois le dépannage terminé, revenez au niveau Information (la journalisation de toutes les informations peut générer des fichiers journaux très volumineux).

Exécuter une détection
Permet aux utilisateurs de spécifier le dossier où effectuer une analyse pour trouver les menaces.

1. Sélectionnez **Exécuter une détection > Spécifier le dossier**.
2. Sélectionnez le dossier à analyser, puis cliquez sur **OK**. Toutes les menaces détectées s'affichent dans l'interface utilisateur de l'agent.

Gestion des menaces
Permet aux utilisateurs de supprimer les fichiers *mis en quarantaine* du périphérique.

1. Sélectionnez **Gestion des menaces > Supprimer les fichiers mis en quarantaine**.
2. Cliquez sur **OK** pour confirmer.

Machines virtuelles

Vous devez suivre certaines recommandations lorsque vous utilisez l'agent Threat Defense sur une image de machine virtuelle.

Lorsque vous créez une image de machine virtuelle afin de l'utiliser comme modèle, déconnectez les paramètres réseau de la machine virtuelle avant d'installer l'agent. Cela empêche l'agent de communiquer avec la console et de configurer les détails du périphérique. Vous évitez ainsi de créer des périphériques en double dans la console.

Désinstallation protégée par un mot de passe

PARAMÈTRES > Application

Les administrateurs peuvent exiger un mot de passe pour la désinstallation de l'agent. Pour désinstaller l'agent avec un mot de passe :

- Si l'installation a été réalisée avec le programme d'installation MSI, désinstallez le logiciel avec le MSI ou utilisez le Panneau de configuration.
- Si l'installation a été réalisée avec le programme d'installation EXE, utilisez ce même EXE pour la désinstallation. Le Panneau de configuration ne fonctionne pas si l'installation a été réalisée avec le programme d'installation EXE et qu'un mot de passe est requis pour la désinstallation.
- Si vous effectuez la désinstallation via la ligne de commande, ajoutez la chaîne de désinstallation suivante : **`UNINSTALLKEY = [MyUninstallPassword]`**.

Pour créer un mot de passe de désinstallation

1. Connectez-vous à la console (http://dellthreatdefense.com) à l'aide d'un compte administrateur.
2. Sélectionnez **Paramètres > Application**.
3. Cochez la case **Exiger un mot pour la désinstallation de l'agent**.
4. Entrez le mot de passe.
5. Cliquez sur **Enregistrer**.

Intégrations

La console Threat Defense permet l'intégration avec certains programmes tiers.

Syslog/SIEM

Threat Defense peut s'intégrer au logiciel Security Information Event Management (SIEM) grâce à la fonction Syslog. Les événements Syslog sont conservés tant que les événements d'agent persistent dans la console.

Pour connaître les adresses IP les plus récentes pour les messages Syslog, contactez le support Dell.

Types d'événement

Journal d'audit

Sélectionnez cette option pour envoyer le journal d'audit des actions réalisées par les utilisateurs dans la console (site Web) au serveur Syslog. Les événements du journal d'audit apparaissent toujours dans l'écran Journal d'audit, même si vous désélectionnez cette option.

Exemple de message de journal d'audit transmis à Syslog

Périphériques

Sélectionnez cette option pour envoyer les événements de périphérique au serveur Syslog.

- Lorsqu'un nouveau périphérique est inscrit, le programme reçoit deux messages pour cet événement : Inscription et Sécurité du système.

  Exemple de message pour l'événement Périphérique inscrit

- Lorsque vous supprimez un périphérique.

  Exemple de message pour l'événement Périphérique supprimé

- Lorsque vous modifiez la stratégie, la zone, le nom ou le niveau de journalisation d'un périphérique.

  Exemple de message pour l'événement Périphérique mis à jour

Menaces

Sélectionnez cette option pour consigner toutes les nouvelles menaces détectées et tous les changements concernant une menace existante sur le serveur Syslog. Les modifications incluent la définition d'une menace comme *supprimée*, *mise en quarantaine*, *ignorée* ou *exécutée*.

Il existe 5 types d'événement de menace :

- **threat_found** : une nouvelle menace a été détectée avec l'état *Dangereux*.
- **threat_removed** : une menace existante a été *supprimée*.
- **threat_quarantined** : une nouvelle menace a été détectée avec l'état *Quarantaine*.
- **threat_waived** : une nouvelle menace a été détectée avec l'état *Ignoré*.
- **threat_changed** : le comportement d'une menace existante a changé (exemples : Score, État de quarantaine, État d'exécution).
- **threat_cleared** : une menace qui a été ignorée, ajoutée à la liste de confiance ou supprimée de la quarantaine sur un périphérique.

Exemple de message pour un événement de menace

Classification des menaces
Des centaines de menaces sont classifiées chaque jour comme Programme malveillant ou PUP (Programme potentiellement indésirable). Si vous sélectionnez cette option, vous vous abonnez aux notifications concernant ces événements.

Exemple de message de classification de menace

SIEM (Security Information and Event Management)
Spécifie le type de serveur Syslog ou SIEM auquel les événements doivent être envoyés.

Protocole
Cette valeur doit être identique à celle configurée sur votre serveur Syslog. Valeurs disponibles : UDP et TCP. UDP est généralement déconseillé, car il ne garantit pas la distribution des messages. Dell vous recommande TCP (valeur par défaut).

TLS/SSL
Disponible uniquement si le protocole choisi est TCP. TLS/SSL garantit que le message Syslog est crypté pour le transit de Threat Defense vers le serveur Syslog. Dell encourage ses clients à activer cette option. Vérifiez que le serveur Syslog est configuré pour écouter les messages TLS/SSL.

Adresse IP/Domaine
Spécifie l'adresse IP ou le nom de domaine entièrement qualifié (FQDN) du serveur Syslog configuré par le client. Consultez vos experts réseau en interne pour vous assurer que les paramètres de pare-feu et de domaine sont correctement configurés.

Port
Spécifie le numéro du port des périphériques où le serveur Syslog écoute les messages. Il doit s'agir d'un nombre entre 1 et 65535. Valeurs courantes : 512 pour UDP, 1235 ou 1468 pour TCP et 6514 pour Secured TCP (exemple : TCP avec option TLS/SSL activée).

Gravité
Spécifie la gravité des messages à afficher sur le serveur Syslog. Ce champ est subjectif. Choisissez le niveau que vous préférez. La valeur de gravité ne change pas les messages retransmis à Syslog.

Site
Spécifie le type d'application qui journalise le message. Valeur par défaut : Interne (ou Syslog). Cette option permet de trier les messages lorsque le serveur Syslog les reçoit.

Test de la connexion
Cliquez sur **Tester la connexion** pour tester les paramètres IP/Domaine, Port et Protocole. Si vous avez entré des valeurs valides, une confirmation indiquant la *réussite* s'affiche au bout d'un instant.

Authentification personnalisée

Utilisez des IdP (Identity Providers, fournisseurs d'identité) externes pour vous connecter à la console. Pour cela, vous devez configurer des paramètres avec votre IdP afin d'obtenir un certificat X.509 et une URL pour la vérification de votre connexion IdP. L'authentification personnalisée fonctionne avec Microsoft SAML 2.0. Nous avons vérifié : cette option fonctionne avec OneLogin, OKTA, Microsoft Azure et PingOne. Cette fonction comporte aussi le paramètre Personnalisé, et devrait fonctionner avec tous les autres fournisseurs d'identité qui suivent Microsoft SAML 2.0.

Remarque : l'authentification personnalisée ne prend pas en charge Active Directory Federation Services (ADFS).

- **Authentification complexe** : fournit un accès avec authentification multifacteur.
- **Authentification unique** : fournit un accès avec authentification unique (SSO).

  Remarque : le choix de l'authentification complexe ou de l'authentification unique n'affecte pas les paramètres d'authentification personnalisée, car tous les paramètres de configuration sont gérés par le fournisseur d'identité (IdP).
- **Autoriser la connexion par mot de passe** : sélectionnez cette option pour autoriser la connexion directe à la console avec authentification unique (SSO). Cela permet d'autoriser les tests SSO sans que l'utilisateur soit bloqué hors de la console. Une fois connecté avec succès à la console par SSO, Dell vous recommande de désactiver cette fonction.
- **Fournisseur :** sélectionnez le fournisseur de services pour l'authentification personnalisée.
- **Certificat X.509** : entrez les informations de certification X.509.
- **URL de connexion** : indiquez l'URL d'authentification personnalisée.

Rapport des données de menace

Feuille de calcul qui contient les informations suivantes concernant l'entreprise :

- **Menaces** : répertorie toutes les menaces détectées dans l'entreprise. Ces informations incluent le nom et l'état du fichier (*Dangereux*, *Anormal*, *Ignoré* et *Mis en quarantaine*).
- **Unités** : répertorie tous les périphériques de l'entreprise où l'agent Threat Defense est installé. Ces informations incluent le nom du périphérique, la version de son système d'exploitation et celle de l'agent, et la stratégie appliquée.
- **Indicateurs de menace** : répertorie chaque menace, avec ses caractéristiques.
- **Effacé** : répertorie tous les fichiers qui ont été *effacés* de votre entreprise. Ces informations comprennent des fichiers *ignorés*, ajoutés à la *liste de confiance* ou *supprimés* du dossier *Quarantaine* d'un périphérique.
- **Événements** : répertorie tous les événements liés au diagramme Événements de menace du tableau de bord, pour les 30 derniers jours. Ces informations incluent la valeur de hachage, le nom du périphérique, le chemin du fichier et la date à laquelle l'événement s'est produit.

Lorsque cette fonction est activée, le rapport est automatiquement mis à jour à 1h00 du matin, Heure standard du Pacifique (PST). Cliquez sur **Régénérer le rapport** pour générer manuellement une mise à jour.

Le rapport des données de menaces contient une URL et un jeton que vous pouvez utiliser pour télécharger le rapport sans avoir besoin de vous connecter à la console. Il est également possible de supprimer ou de régénérer le jeton, selon les besoins, ce qui permet de contrôler les personnes autorisées à accéder au rapport.

DÉPANNAGE

Cette section présente la liste de questions auxquelles vous devez répondre et celle des fichiers à collecter pour le dépannage des incidents Threat Defense. Ces informations permettront au support Dell de vous aider à résoudre le problème.

Cette section répertorie également certains problèmes courants, avec des suggestions de solution.

Support

Paramètres d'installation

- Quelle est la méthode d'installation ? Indiquez tous les paramètres utilisés.
    - Exemple – Windows : utilisation de LAUCHAPP=0 pour l'installation depuis la ligne de commande, afin de masquer l'icône de l'agent et le dossier du menu Démarrer lors de l'exécution.
    - Exemple - macOS : utilisation de SelfProtectionLevel=1 pour l'installation depuis la ligne de commande pour désactiver l'autoprotection (Self Protection) sur l'agent.
- Quelles étapes d'installation avez-vous suivies ?
    - Exemple – Windows : avez-vous utilisé le programme d'installation MSI ou EXE ?
    - Exemple – Tous les systèmes d'exploitation : avez-vous utilisé des options de ligne de commande ? Par exemple Mode silencieux ou Pas d'interface utilisateur d'agent.
- Activez la journalisation détaillée pour l'installation.

Problèmes de performances

- Prenez une capture d'écran de Gestionnaire de tâches (Windows) ou de Moniteur d'activité (macOS), montrant les processus et la consommation de mémoire de Threat Defense.
- Capturez un fichier de vidage (dump) du processus Threat Defense.
- Collectez les journaux de débogage.
- Collectez la sortie Informations système au moment de l'incident.
    - Sous Windows : msinfo32 ou winmsd
    - Pour macOS : Informations système
- Collectez tous les journaux d'événements (Windows) ou toutes les informations de console (macOS) pertinents.

Problèmes de mise à jour, d'état et de connexion

- Vérifiez que le port 443 est ouvert dans le pare-feu, et que le périphérique parvient à résoudre les adresses des sites Cylance.com et à s'y connecter.
- Le périphérique apparaît-il dans la page Périphériques de la console ? Est-il en ligne ou hors ligne ? Quelle est l'heure de sa dernière connexion ?
- Le périphérique utilise-t-il un proxy pour se connecter à Internet ? Les références d'identification sont-elles correctement configurées sur le proxy ?
- Redémarrez le service Threat Defense pour qu'il tente de se connecter à la console.
- Collectez les journaux de débogage.
- Collectez la sortie Informations système au moment de l'incident.
    - Sous Windows : msinfo32 ou winmsd
    - Pour macOS : Informations système

Activation des journaux de débogage

Par défaut, Threat Defense conserve les fichiers journaux stockés dans **`C:\Program Files\Cylance\Desktop\log`**. Pour le dépannage, Threat Defense peut être configuré pour produire des journaux plus détaillés (verbose).

Incompatibilités de Contrôle des scripts

Problème :

Lorsque Contrôle des scripts est activé sur certains périphériques, il peut provoquer des conflits avec d'autres logiciels exécutés sur ces périphériques. Le conflit est généralement dû au fait que l'agent injecte des données dans des processus appelés par d'autres logiciels.

Solution :

Selon le logiciel concerné, vous pouvez résoudre le problème en ajoutant des exclusions de processus spécifiques à la stratégie de périphérique dans la console. Autre option : activez le mode de compatibilité (clé de registre) sur chacun des périphériques concernés. Cependant, si les exclusions ne suffisent pas, Dell vous recommande de désactiver Contrôle des scripts dans la stratégie de périphérique appliquée aux périphériques concernés. Cela devrait restaurer le fonctionnement normal de ces périphériques.

Remarque : cette solution basée sur le mode de compatibilité s'adresse uniquement à la version 1370 de l'agent. À partir de la version 1382 de l'agent, le processus d'injection a été mis à jour pour garantir la compatibilité avec d'autres produits.

Mode de compatibilité

Ajoutez la clé de registre suivante pour activer le mode de compatibilité :

1. Dans l'Éditeur de registre de l'ordinateur, accédez à **`HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`**.
2. Cliquez avec le bouton droit de la souris sur **Bureau**, cliquez sur **Autorisation**, puis désignez-vous comme propriétaire et attribuez-vous le droit **Contrôle total**. Cliquez sur **OK**.
3. Effectuez un clic droit sur **Bureau**, puis sélectionnez **Nouveau > Valeur binaire**.
4. Nommez le fichier **Mode de compatibilité**.
5. Ouvrez le paramètre de registre et changez la valeur en **01**.
6. Cliquez sur **OK**, puis fermez l'Éditeur de registre.
7. Vous devrez peut-être redémarrer le périphérique.

Options de ligne de commande

Avec Psexec :

```
psexec -s reg add HKEY_LOCAL_MACHINE\SOFTWARE
\Cylance\Desktop /v CompatibilityMode /t REG_BINARY /d 01
```

Pour exécuter une commande sur plusieurs périphériques, utilisez la sous-commande **`Invoke-Command cmdlet`**:

```
$servers = "testComp1","testComp2","textComp3"

$credential = Get-Credential -Credential {UserName}\administrator

Invoke-Command -ComputerName $servers -Credential $credential -
ScriptBlock {New-Item -Path HKCU:\Software\Cylance\Desktop -Name
CompatibilityMode -Type REG_BINARY -Value 01}
```

ANNEXE A : GLOSSAIRE

Anormal	Fichier suspect avec un score plus faible (1 à 59), peu susceptible d'être un programme malveillant
Administrateur	Gestionnaire locataire pour Threat Defense
Agent	Hôte de point de terminaison Threat Defense, qui communique avec la console
Journal d'audit	Journal qui consigne les actions exécutées depuis la console Threat Defense
Quarantaine auto	Empêcher automatiquement l'exécution de tous les fichiers *dangereux* et/ou *anormaux*
Téléchargement auto	Télécharger automatiquement tous les fichiers Portable Executable (PE) inconnus, identifiés comme *dangereux* ou *anormaux*, sur le cloud Cylance Infinity pour analyse.
Guide d'utilisation de la console	Interface utilisateur de gestion de Threat Defense
Stratégie de périphérique	Stratégie Threat Defense que l'administrateur de l'entreprise peut configurer pour déterminer la façon dont les menaces sont traitées sur tous les périphériques
Quarantaine globale	Interdit l'exécution d'un fichier au niveau global (sur tous les périphériques de l'entreprise)
Liste de confiance globale	Autorise l'exécution d'un fichier au niveau global (sur tous les périphériques de l'entreprise)
Infinity	Modèle mathématique utilisé pour attribuer un score aux fichiers
Organisation	Compte de locataire qui utilise le service Threat Defense
Mettre en quarantaine	Interdire l'exécution d'un fichier au niveau local (sur un périphérique spécifique)
Menaces	Fichiers potentiellement malveillants, que Threat Defense a détectés et classés comme *dangereux* ou *anormaux*
Dangereux	Fichier suspect avec un score élevé (60 à 100), susceptible d'être un programme malveillant
Ignorer	Autoriser l'exécution d'un fichier au niveau local (sur un périphérique spécifique)
Zone	Méthode d'organisation et de regroupement des périphériques dans l'entreprise, sur la base de la priorité, des fonctions, etc.
Règle de zone	Fonction qui permet d'automatiser l'attribution des périphériques à des zones spécifiques, sur la base des adresses IP, du système d'exploitation ou du nom de périphérique.

ANNEXE B : GESTION DES EXCEPTIONS

Il arrive que les utilisateurs aient besoin de *mettre en quarantaine* ou d'*autoriser* (*ignorer*) manuellement un fichier. Threat Defense permet de gérer des exceptions pour chaque périphérique (*local*), pour un groupe de périphériques (*stratégie*) ou pour toute l'entreprise (*global*).

Fichiers

Local : *mettre en quarantaine* ou *ignorer* (*liste de confiance*) un fichier sur le périphérique. Cela s'avère utile pour *bloquer* ou *autoriser* temporairement un fichier jusqu'à un moment plus propice pour l'analyser. Le fait d'*ignorer* un fichier sur un périphérique est également utile lorsqu'il s'agit du seul périphérique sur lequel le fichier doit être autorisé à *s'exécuter*. Dell préconise l'utilisation d'une *stratégie* ou d'une *liste globale* lorsque cette action a besoin d'être effectuée sur plusieurs périphériques.

Stratégie : *mettre en liste de confiance* un fichier sur tous les périphériques attribués à une stratégie. Cette option est utile pour autoriser un fichier sur un groupe de périphériques (par exemple, pour autoriser les périphériques IT à exécuter des outils susceptibles de servir des objectifs malveillants, comme PsExec). Il est impossible de *mettre en quarantaine* un fichier au niveau Stratégie.

Global : *mettre en quarantaine* ou *en liste de confiance* un fichier pour toute l'entreprise. *Mettre en quarantaine* un fichier malveillant dans l'entreprise. *Mettre en liste de confiance* un fichier connu pour être sain et utilisé dans l'entreprise, mais que l'agent identifie comme malveillant.

Scripts

Stratégie : le contrôle des scripts permet d'approuver l'exécution des scripts depuis un dossier spécifique. En autorisant les scripts à s'exécuter depuis un dossier, vous les autorisez aussi à s'exécuter depuis tous les sous-dossiers.

Certificats

Global : ajouter des certificats à la console, puis à la *liste de confiance globale*. Cela permet aux applications signées par ce certificat de s'exécuter dans l'entreprise.

Pour ajouter un certificat, sélectionnez **Paramètres > Certificats**, puis cliquez sur **Ajouter un certificat**.

Pour ajouter le certificat à la *liste de confiance globale*, sélectionnez **Paramètres > Liste globale**, accédez à l'onglet **Liste de confiance globale** puis à l'onglet **Certificats**, puis cliquez sur **Ajouter un certificat**.

ANNEXE C : AUTORISATIONS UTILISATEUR

Les actions que les utilisateurs peuvent exécuter dépendent des autorisations utilisateur (rôle) qui leur ont été attribuées. En général, les utilisateurs Administrateur peuvent réaliser des actions dans l'ensemble de l'entreprise. Les utilisateurs Gestionnaire de zone et Utilisateur sont limités aux zones qui leur sont attribuées. Cette restriction signifie qu'ils ne peuvent accéder qu'aux périphériques de la zone en question et ne voient que les données de menace relatives à ces périphériques. Si un gestionnaire de zone ou un utilisateur ne voit pas un périphérique ou une menace spécifique, cela signifie probablement que le périphérique concerné n'appartient pas aux zones attribuées à ces personnes.

	UTILISATEUR	GESTIONNAIRE DE ZONE	ADMIN
Mise à jour de l'agent			
Afficher/Modifier			X
Journaux d'audit			
Afficher			X
Périphériques			
Ajouter des périphériques – Global			X
Ajouter des périphériques à une zone			X
Supprimer des périphériques – Global			X
Supprimer des périphériques d'une zone		X	X
Renommer un périphérique		X	X
Zones			
Créer une zone			X
Supprimer une zone			X
Renommer une zone – Partout			X
Renommer une zone qui lui est attribuée		X	X
Stratégie			
Créer une stratégie – Global			X
Créer une stratégie pour une zone			X

	UTILISATEUR	GESTIONNAIRE DE ZONE	ADMIN
Ajouter une stratégie – Global			X
Ajouter une stratégie à une zone		X	X
Supprimer une stratégie – Global			X
Supprimer une stratégie d'une zone		X	X
Menaces			
Mettre des fichiers en quarantaine – Global			X
Mettre des fichiers en quarantaine dans une zone	X	X	X
Ignorer des fichiers – Global			X
Ignorer des fichiers dans une zone	X	X	X
Quarantaine globale/Liste de confiance globale			X
Paramètres			
Générer ou supprimer un jeton d'installation			X
Générer ou supprimer une URL d'invitation			X
Copier un jeton d'installation	X	X	X
Copier une URL d'invitation			X
Gestion des utilisateurs			
Attribuer des utilisateurs à n'importe quelle zone			X
Attribuer des utilisateurs à une zone qu'il gère		X	X
Désigner un gestionnaire de zone – Global			X
Désigner un gestionnaire de zone pour les zones qu'il gère		X	X
Supprimer des utilisateurs de la console			X
Supprimer des utilisateurs d'une zone – Global			X
Supprimer des utilisateurs d'une zone qu'il gère		X	X

ANNEXE D : FILTRE D'ÉCRITURE BASÉ SUR DES FICHIERS

L'agent Dell Threat Defense peut être installé sur un système exécutant Windows Embedded Standard 7 (client léger, « Thin Client »). Sur les périphériques intégrés, il est possible que l'écriture sur le stockage du système ne soit pas autorisée. Dans ce cas, le système peut utiliser un filtre d'écriture basé sur des fichiers (FBWF) pour rediriger les éventuelles écritures sur le stockage du système vers le cache de la mémoire du système. Cela peut entraîner des problèmes, notamment de perte des modifications par l'agent au redémarrage du système.

Lorsque vous utilisez l'agent sur un système intégré, procédez comme suit :

1. Avant d'installer l'agent, désactivez le filtre d'écriture basé sur des fichiers à l'aide de la commande suivante : `fbwfmgr /disable`.
2. Redémarrez le système. Cela permet d'appliquer la désactivation du filtre d'écriture basé sur des fichiers.
3. Installez l'agent Dell Threat Defense.

4. Après l'installation de l'agent, réactivez le filtre d'écriture basé sur des fichiers à l'aide de la commande suivante : `fbwfmgr /enable`.
5. Redémarrez le système. Cela permet d'appliquer l'activation du filtre d'écriture basé sur des fichiers.
6. Dans le filtre d'écriture basé sur des fichiers, excluez les dossiers suivants :
    a. C:\Program Files\Cylance\Desktop ; l'exclusion de ce dossier permet aux mises à jour de l'agent d'être conservées après un redémarrage du système.
7. Utilisez la commande suivante pour exclure le dossier Bureau : `fbwfmgr /addexclusion C: "\Program Files\Cylance\Desktop\"`
    a. Ces informations partent du principe que vous effectuez l'installation dans le répertoire par défaut. Remplacez l'exclusion par le dossier dans lequel vous avez installé l'agent, le cas échéant.
8. Si vous envisagez de stocker les menaces sur la machine pour effectuer des tests sur l'agent, prenez soin d'exclure également l'emplacement de stockage du filtre d'écriture basé sur des fichiers (`C:\Samples` par exemple).