Portail de gestion

24.03

Guide de l'Administrateur d'entreprise

RÉVISION : 11/04/2024

Table des matières

À propos de ce document

Ce document est conçu pour les administrateurs client qui souhaitent se servir du portail de gestion Cloud pour créer et gérer les comptes, les unités et les quotas des utilisateurs, configurer et contrôler les accès, et surveiller l'utilisation et les opérations dans leur organisation Cloud.

À propos du portail de gestion

Le portail de gestion est une interface Web de la plate-forme Cloud qui fournit des services de protection de données.

Alors que chaque service possède sa propre interface Web, appelée Console de service, le portail de gestion permet aux administrateurs de contrôler l'utilisation des services, de créer des comptes utilisateur et des unités, de générer des rapports, et bien plus.

Comptes et unités

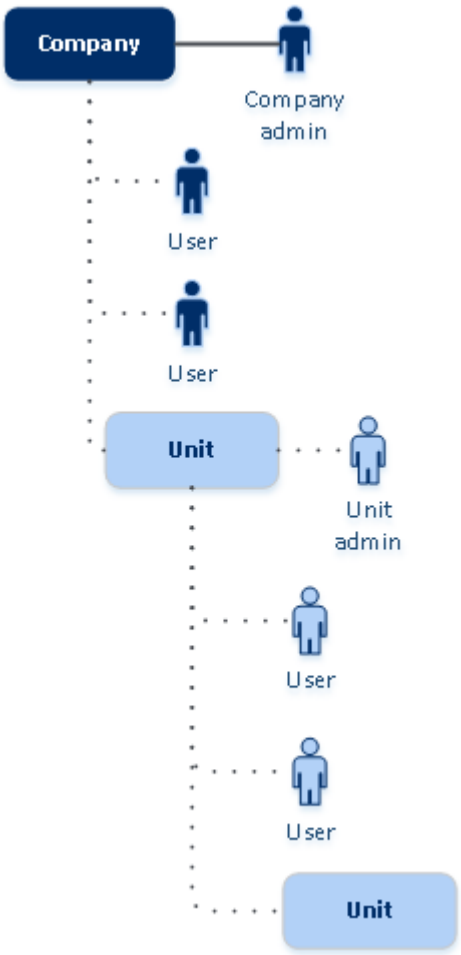
Il existe deux types de comptes utilisateur : les comptes administrateur et les comptes utilisateur.

- Les **administrateurs** ont accès au portail de gestion. Ils possèdent le rôle d'administrateur dans tous les services.
- Les **utilisateurs** n'ont pas accès au portail de gestion. Leur accès aux services et leurs rôles dans ces services sont définis par un administrateur.

Les administrateurs peuvent créer des unités, qui correspondent généralement à des unités ou des départements de l'organisation. Chaque compte existe soit au niveau de la société, soit dans une unité.

Un administrateur peut gérer des unités, des comptes administrateur et des comptes utilisateur de même niveau ou hiérarchiquement inférieurs.

Le diagramme ci-dessous présente trois niveaux de hiérarchie : la société et deux unités. Les unités et les comptes facultatifs sont signalés par une ligne en pointillés.



Le tableau ci-dessous résume les opérations pouvant être effectuées par les administrateurs et les utilisateurs.

Opération	Utilisateurs	Administrateurs
Créer des unités	Non	Oui
Créer des comptes	Non	Oui
Téléchargez et installez le logiciel	Oui	Oui
Utilisez les services	Oui	Oui
Créer des rapports concernant l'utilisation du service	Non	Oui

Gestion des quotas

Les quotas limitent les possibilités d'utilisation du service par le tenant.

Dans votre portail de gestion, vous pouvez afficher les quotas de service que votre fournisseur de service a alloués à votre organisation, mais vous ne pouvez pas les gérer.

Vous pouvez gérer les quotas de service pour vos utilisateurs.

Afficher les quotas pour votre organisation

Dans le portail de gestion, accédez à **Vue d'ensemble** > **Utilisation**. Vous verrez un tableau de bord affichant les quotas alloués à votre organisation. Les quotas pour chaque service s'affichent dans un onglet différent.

Quotas de sauvegarde

Indiquez le quota de stockage dans le Cloud, le quota de sauvegarde au niveau local et le nombre maximum de machines/terminaux/sites Web qu'un utilisateur est autorisé à protéger. Les quotas suivants sont disponibles.

Quotas pour les terminaux

- **Postes de travail**
- **Serveurs**
- **Machines virtuelles**
- **Terminaux mobiles**
- **Serveurs d'hébergement Web** (Serveurs physiques et virtuels Linux qui exécutent des panneaux de configuration cPanel, Plesk, DirectAdmin, VirtualMin ou ISPManager)
- **Sites Web**

Une machine, un terminal ou un site Web sont considérés comme protégés tant qu'au moins un plan de protection leur est appliqué. Un terminal mobile devient protégé après la première sauvegarde.

Lorsque le dépassement du quota de terminaux est atteint, l'utilisateur ne peut plus activer de plans de protection sur d'autres terminaux.

Quotas pour les sources de données Cloud

- **Postes Microsoft 365**

  Ce quota est appliqué par le fournisseur de services à l'ensemble de l'entreprise. Les administrateurs de l'entreprise peuvent afficher le quota et l'utilisation dans le portail de gestion.

  Les licences des postes Microsoft 365 dépendent du mode de facturation sélectionné pour Cyber Protection.

Important
L'agent local et l'agent dans le cloud consomment des quotas distincts. Si vous sauvegardez les mêmes ressources à l'aide des deux agents, vous êtes facturé deux fois. Par exemple :

- Si vous sauvegardez les boîtes aux lettres de 120 utilisateurs à l'aide de l'agent local et les fichiers OneDrive de ces mêmes utilisateurs à l'aide de l'agent dans le cloud, vous êtes facturé pour 240 postes Microsoft 365.
- Si vous sauvegardez les boîtes aux lettres de 120 utilisateurs à l'aide de l'agent local et également à l'aide de l'agent dans le cloud, vous êtes facturé pour 240 postes Microsoft 365.

En mode de facturation **Par ressource**, le quota de **Postes Microsoft 365** est comptabilisé par utilisateurs uniques. Un utilisateur unique est un utilisateur qui dispose d'au moins l'un des éléments suivants :

- Boîte aux lettres protégée
- OneDrive protégé
- Accès à au moins une ressource protégée de l'entreprise : Site Microsoft 365 SharePoint Online ou Microsoft 365 Teams.
  Pour apprendre à contrôler le nombre de membres d'un site Microsoft 365 SharePoint ou Teams, reportez-vous à cet article de la base de connaissances.

Remarque
Les utilisateurs Microsoft 365 bloqués qui ne disposent pas d'une boîte aux lettres personnelle protégée ou de OneDrive, et n'ont accès qu'à des ressources partagées (boîtes aux lettres partagées, sites SharePoint et Microsoft Teams) ne sont pas chargés.
Les utilisateurs bloqués sont ceux qui n'ont pas d'informations de connexion valides et ne peuvent pas accéder aux services Microsoft 365. Pour savoir comment bloquer tous les utilisateurs sans licence d'une organisation Microsoft 365, voir "Empêcher les utilisateurs de Microsoft 365 sans licence de se connecter" (p. 11).

Les postes Microsoft 365 suivants ne font pas l'objet d'une facturation et ne nécessitent pas de licence par poste :

- Boîtes aux lettres partagées
- Salles et équipement
- Utilisateurs externes avec accès aux sites SharePoint et/ou équipes Microsoft Teams sauvegardés

Pour plus d'informations sur les options de licence avec le mode de facturation par gigaoctet, reportez-vous à Cyber Protect Cloud: Microsoft 365 per GB licensing.
Pour plus d'informations sur les options de licence avec le mode de facturation par ressource, reportez-vous à Cyber Protect Cloud: Microsoft 365 licensing and pricing changes.

- **Microsoft 365 Teams**
  Ce quota est appliqué par le fournisseur de services à l'ensemble de l'entreprise. Ce quota active ou désactive la capacité à protéger des équipes Microsoft 365 Teams et définit le nombre

maximum d'équipes pouvant être protégées. Pour la protection d'une équipe, quel que soit le nombre de membres ou de canaux, un quota est nécessaire. Les administrateurs de l'entreprise peuvent afficher le quota et l'utilisation dans le portail de gestion.

- **Microsoft 365 SharePoint Online**

  Ce quota est appliqué par le fournisseur de services à l'ensemble de l'entreprise. Ce quota active ou désactive la capacité à protéger des sites SharePoint Online et définit le nombre maximum de collections de sites et de sites de groupe pouvant être protégés.

  Les administrateurs de l'entreprise peuvent afficher le quota dans le portail de gestion. Ils peuvent également consulter le quota, ainsi que la quantité de stockage occupée par les sauvegardes SharePoint Online, dans les rapports d'utilisation.
- **Postes Google Workspace**

  Ce quota est appliqué par le fournisseur de services à l'ensemble de l'entreprise. L'entreprise peut être autorisée à protéger des boîtes aux lettres **Gmail** (y compris des agendas et des contacts), des fichiers **Google Drive** ou les deux. Les administrateurs de l'entreprise peuvent afficher le quota et l'utilisation dans le portail de gestion.
- **Drive partagé Google Workspace**

  Ce quota est appliqué par le fournisseur de services à l'ensemble de l'entreprise. Ce quota active ou désactive la capacité à protéger des Drive partagés Google Workspace. Si le quota est activé, un nombre illimité de Drive partagés peut être protégé. Les administrateurs de l'entreprise ne peuvent pas consulter le quota dans le portail de gestion, mais peuvent consulter la quantité de stockage occupée par les sauvegardes de Drive partagé dans les rapports d'utilisation.

  La sauvegarde de Drive partagés Google Workspace n'est disponible que pour les clients qui disposent d'au moins un quota de postes Google Workspace en plus. Ce quota est uniquement vérifié et ne sera pas utilisé.

Un poste Microsoft 365 est considéré comme protégé si au moins un plan de protection est appliqué à la boîte aux lettres ou au OneDrive de l'utilisateur. Un poste Google Workspace est considéré comme protégé si au moins un plan de protection est appliqué à la boîte aux lettres ou au Google Drive de l'utilisateur.

Lorsque le dépassement du quota de postes est atteint, un administrateur d'entreprise ne peut plus activer de plans de protection sur d'autres postes.

Quotas pour le stockage

- **Sauvegarde locale**

  Le quota **Sauvegarde locale** limite la taille totale des sauvegardes locales créées à l'aide de l'infrastructure Cloud. Aucun dépassement ne peut être défini pour ce quota.
- **Ressources Cloud**

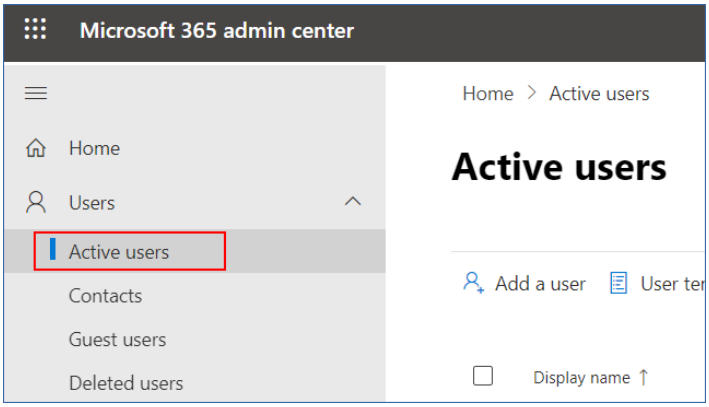
  Le quota de **ressources Cloud** combine le quota de stockage de sauvegarde et le quota de reprise d'activité après sinistre. Le quota de stockage des sauvegardes limite la taille totale des sauvegardes situées dans le stockage dans le Cloud. Lorsque le dépassement de quota de stockage de sauvegarde est dépassé, la sauvegarde échoue.

Empêcher les utilisateurs de Microsoft 365 sans licence de se connecter

Vous pouvez empêcher tous les utilisateurs sans licence de votre organisation Microsoft 365 de se connecter en modifiant leur statut de connexion.

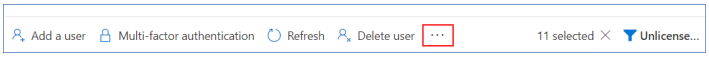
Pour empêcher les utilisateurs sans licence de se connecter

1. Connectez-vous au centre d'administration de Microsoft 365 (https://admin.microsoft.com) en tant qu'administrateur général.
2. Dans le menu de navigation, accédez à **Utilisateurs** > **Utilisateurs actifs**.



3. Cliquez sur **Filtre**, puis sélectionnez **Utilisateurs sans licence**.

4. Cochez les cases situées à côté des noms d'utilisateurs, puis cliquez sur l'icône en forme de points de suspension (...).



5. Dans le menu, sélectionnez **Modifier l'état de connexion**.
6. Cochez la case **Empêcher la connexion d'utilisateurs**, puis cliquez sur **Enregistrer**.

Quotas de reprise d'activité après sinistre

Remarque
Les éléments de reprise d'activité après sinistre ne sont disponibles qu'avec le module complémentaire de reprise d'activité après sinistre.

Ces quotas sont appliqués par le fournisseur de services à l'ensemble de l'entreprise. Les administrateurs de l'entreprise peuvent afficher les quotas et l'utilisation dans le portail de gestion, mais ne peuvent pas définir de quotas pour un utilisateur.

- **Stockage pour la reprise d'activité après sinistre**
  Le stockage de reprise d'activité après sinistre affiche la taille du stockage des sauvegardes des serveurs protégés avec la reprise d'activité après sinistre. L'utilisation du stockage de reprise d'activité après sinistre correspond à l'utilisation du stockage des sauvegardes des ressources

protégées avec des serveurs de reprise d'activité après sinistre. Ce stockage est calculé à partir du moment où un serveur de restauration est créé, qu'il soit en cours d'exécution ou non. Si le quota est dépassé, il ne sera pas possible de créer des serveurs primaires et de restauration, ni d'ajouter/étendre des disques des serveurs primaires existants. Si la surconsommation de ce quota est dépassée, il ne sera pas possible d'initier un basculement ni de démarrer un serveur arrêté. Les serveurs en cours d'exécution continuent à fonctionner.

- **Points de calcul**

  Ce quota limite les ressources processeur et les ressources RAM utilisées par les serveurs primaires et de restauration pendant une période de facturation. Si le quota est atteint, tous les serveurs primaires et de restauration sont coupés. Ces serveurs ne pourront plus être utilisés avant le début de la prochaine période de facturation. La période de facturation par défaut est un mois complet.

  Lorsque le quota est désactivé, les serveurs ne peuvent pas être utilisés, quelle que soit la période de facturation.
- **Adresses IP publiques**

  Ce quota limite le nombre d'adresses IP publiques qui peuvent être attribuées à des serveurs primaires et de restauration. Si le quota est atteint, il n'est pas possible d'activer des adresses IP publiques pour d'autres serveurs. Vous pouvez interdire à un serveur d'utiliser une adresse IP publique en désactivant la case à cocher **Adresse IP publique** dans les paramètres du serveur. Après cela, vous pouvez autoriser un autre serveur à utiliser une adresse IP publique, qui ne sera généralement pas la même.

  Lorsque le quota est désactivé, tous les serveurs cessent d'utiliser des adresses IP publiques et ne sont donc plus accessibles depuis Internet.
- **Serveurs Cloud**

  Ce quota limite le nombre total de serveurs primaires et de restauration. Si le quota est atteint, il n'est pas possible de créer des serveurs primaires ou de restauration.

  Lorsque le quota est désactivé, les serveurs sont visibles dans la console Cyber Protect, mais seule l'option **Supprimer** est disponible.
- **Accès Internet**

  Ce quota active ou désactive l'accès à Internet à partir de serveurs primaires ou de restauration.

  Lorsque ce quota est désactivé, les serveurs primaires ou de restauration ne peuvent pas établir de connexion à Internet.

Quotas pour la File Sync & Share

Ces quotas sont appliqués par le fournisseur de services à l'ensemble de l'entreprise. Les administrateurs de l'entreprise peuvent afficher les quotas et l'utilisation dans le portail de gestion.

- **Utilisateurs**

  Le quota définit le nombre d'utilisateurs pouvant accéder à ce service.

  Les comptes administrateur ne sont pas comptabilisés dans ce quota.
- **Stockage dans le Cloud**

Il s'agit d'un stockage dans le Cloud, destiné à stocker les fichiers des utilisateurs. Le quota définit l'espace alloué à un tenant dans le stockage dans le Cloud.

Quotas d'envoi de données physiques

Les quotas du service d'envoi de données physiques sont consommés sur une base par lecteur. Vous pouvez enregistrer les sauvegardes initiales de plusieurs machines sur un seul disque dur.

Ces quotas sont appliqués par le fournisseur de services à l'ensemble de l'entreprise. Les administrateurs de l'entreprise peuvent afficher les quotas et l'utilisation dans le portail de gestion, mais ne peuvent pas définir de quotas pour un utilisateur.

- **Vers le Cloud**
  Permet d'envoyer une sauvegarde initiale vers le centre de données du Cloud en utilisant un lecteur de disque dur. Ce quota définit le nombre maximum de lecteurs à transférer vers le centre de données du Cloud.

Quotas pour Notary

Ces quotas sont appliqués par le fournisseur de services à l'ensemble de l'entreprise. Les administrateurs de l'entreprise peuvent afficher les quotas et l'utilisation dans le portail de gestion.

- **Stockage Notary**
  Définit l'espace maximal de stockage dans le cloud des fichiers notariés, des fichiers signés et de ceux dont la notarisation ou la signature est en cours.
  Pour réduire l'utilisation de ce quota, vous pouvez supprimer les fichiers déjà notariés ou signés du stockage de notarisation.
- **Notarisations**
  Définit le nombre maximal de fichiers pouvant être notariés à l'aide du service de notarisation. Un fichier est considéré comme étant notarié dès qu'il est transféré vers le stockage de notarisation et que son état de notarisation passe à **En progrès**.
  Si le même fichier est notarié plusieurs fois, chaque notarisation compte comme une nouvelle.
- **Signatures électroniques**
  Définit le nombre maximal de signatures électroniques numériques.

Quotas principaux pour vos utilisateurs

Les **quotas** vous permettent de limiter la capacité d'un utilisateur à utiliser le service. Pour définir les quotas d'un utilisateur, sélectionnez ce dernier dans l'onglet **Utilisateurs**, sous **Gestion d'entreprise**, puis cliquez sur l'icône en forme de crayon dans la section **Quotas**.

Lorsqu'un quota est dépassé, une notification est envoyée à l'adresse e-mail de l'utilisateur. Si vous ne définissez pas de dépassement de quota, le quota est considéré comme « **souple** ». Cela signifie que les restrictions d'utilisation du service Cyber Protection ne sont pas activées.

Lorsque vous précisez un dépassement de quota, le quota est alors considéré comme « **dur** ». Un **dépassement** permet à un utilisateur de dépasser le quota, selon la valeur indiquée. Lorsque le dépassement est atteint, des restrictions sont appliquées à l'utilisation du service.

Exemple

Quota souple : Vous avez défini le quota des postes de travail sur 20. Lorsque le nombre de postes de travail protégés de l'utilisateur atteint 20, il reçoit une notification par e-mail, mais le service Cyber Protection reste disponible.

Quota dur : Si vous avez défini le quota de postes de travail sur 20 et que le dépassement est de 5, l'utilisateur reçoit alors une notification par e-mail lorsque le nombre de postes de travail protégés atteint 20, et le service Cyber Protection est désactivé lorsque ce nombre atteint 25.

Quotas de sauvegarde

Vous pouvez indiquer le quota de stockage de sauvegarde et le nombre maximum de machines/terminaux/sites Web qu'un utilisateur est autorisé à protéger. Les quotas suivants sont disponibles.

Quotas pour les terminaux

- **Postes de travail**
- **Serveurs**
- **Machines virtuelles**
- **Terminaux mobiles**
- **Serveurs d'hébergement Web** (Serveurs physiques et virtuels Linux qui exécutent des panneaux de configuration cPanel, Plesk, DirectAdmin, VirtualMin ou ISPManager)
- **Sites Web**

Une machine, un terminal ou un site Web sont considérés comme protégés tant qu'au moins un plan de protection leur est appliqué. Un terminal mobile devient protégé après la première sauvegarde.

Lorsque le dépassement du quota de terminaux est atteint, l'utilisateur ne peut plus activer de plans de protection sur d'autres terminaux.

Quota pour le stockage

- **Stockage de sauvegarde**

Le quota de stockage des sauvegardes limite la taille totale des sauvegardes situées dans le stockage dans le Cloud. Lorsque le quota de stockage des sauvegardes est dépassé, les sauvegardes échouent.

Important
L'agent local et l'agent dans le cloud consomment des quotas distincts. Si vous sauvegardez les mêmes ressources à l'aide des deux agents, vous êtes facturé deux fois. Par exemple :

- Si vous sauvegardez les boîtes aux lettres de 120 utilisateurs à l'aide de l'agent local et les fichiers OneDrive de ces mêmes utilisateurs à l'aide de l'agent dans le cloud, vous êtes facturé pour 240 postes Microsoft 365.
- Si vous sauvegardez les boîtes aux lettres de 120 utilisateurs à l'aide de l'agent local et également à l'aide de l'agent dans le cloud, vous êtes facturé pour 240 postes Microsoft 365.

Quotas pour la File Sync & Share

Vous pouvez définir les quotas suivants pour la File Sync & Share pour un utilisateur :

- **Espace de stockage personnel**
  Définit l'espace de stockage dans le cloud alloué aux fichiers d'un utilisateur.

Quotas pour Notary

Vous pouvez définir les quotas suivants pour Notary pour un utilisateur :

- **Stockage Notary**
  Définit l'espace maximal de stockage dans le cloud des fichiers notariés, des fichiers signés et de ceux dont la notarisation ou la signature est en cours.
  Pour réduire l'utilisation de ce quota, vous pouvez supprimer les fichiers déjà notariés ou signés du stockage de notarisation.
- **Notarisations**
  Définit le nombre maximal de fichiers pouvant être notariés à l'aide du service de notarisation. Un fichier est considéré comme étant notarié dès qu'il est transféré vers le stockage de notarisation et que son état de notarisation passe à **En progrès**.
  Si le même fichier est notarié plusieurs fois, chaque notarisation compte comme une nouvelle.
- **Signatures électroniques**
  Définit le nombre maximal de signatures électroniques numériques.

Navigateurs Web pris en charge

L'interface Web prend en charge les navigateurs suivants :

- Google Chrome 29 ou version ultérieure
- Mozilla Firefox 23 ou version ultérieure
- Opera 16 ou version ultérieure
- Microsoft Edge 25 ou version ultérieure
- Safari 8 ou version ultérieure s'exécutant sur les systèmes d'exploitation macOS et iOS

Il est possible que les autres navigateurs (dont les navigateurs Safari s'exécutant sur d'autres systèmes d'exploitation) n'affichent pas correctement l'interface utilisateur ou ne proposent pas certaines fonctions.

Instructions pas-à-pas

Les étapes suivantes vous guideront à travers l'installation et l'utilisation de base du portail de gestion. Elles indiquent comment :

- Activer votre compte administrateur
- Accédez au portail de gestion et aux services
- Créez une unité
- Créez un compte utilisateur

Activation d'un compte administrateur

Après avoir contracté un service, vous recevrez un e-mail contenant les informations suivantes :

- **Votre identifiant.** Nom d'utilisateur que vous utilisez pour vous connecter. Votre identifiant figure également sur la page d'activation du compte.
- Bouton **Activer le compte**. Cliquez sur le bouton et configurez le mot de passe de votre compte. Assurez-vous que le mot de passe contient au moins neuf caractères. Pour plus d'informations sur le mot de passe, reportez-vous à "Exigences relatives au mot de passe" (p. 17).

Exigences relatives au mot de passe

Le mot de passe d'un compte utilisateur doit comporter au moins 9 caractèresLa complexité des mots de passe est également vérifiée et les mots de passe sont classés dans les catégories suivantes :

- Faible
- Moyenne
- Fort

Vous ne pouvez pas enregistrer un mot de passe faible, même s'il contient 9 caractères ou plus. Les mots de passe qui contiennent le nom de l'utilisateur, l'identifiant, l'adresse e-mail de l'utilisateur ou le nom du tenant auquel le compte utilisateur appartient sont toujours considérés comme faibles. La plupart des mots de passe courants sont également considérés comme faibles.

Pour renforcer un mot de passe, ajoutez-lui des caractères. L'utilisation de différents types de caractères (chiffres, majuscules, minuscules et caractères spéciaux) n'est pas obligatoire, mais permet d'obtenir des mots de passe plus forts, mais aussi plus courts.

Accès au portail de gestion et aux services

1. Accédez à la page de connexion de la console de service.
2. Saisissez l'identifiant, puis cliquez sur **Suivant**.
3. Saisissez le mot de passe, puis cliquez sur **Suivant**.

4. Effectuez l'une des actions suivantes :
   - Pour vous connecter au service de sauvegarde, cliquez sur **Portail de gestion**.
   - Pour vous connecter à un service, cliquez sur le nom du service.

Le délai d'expiration pour le portail de gestion est de 24 heures pour les sessions actives et d'une heure pour les sessions inactives.

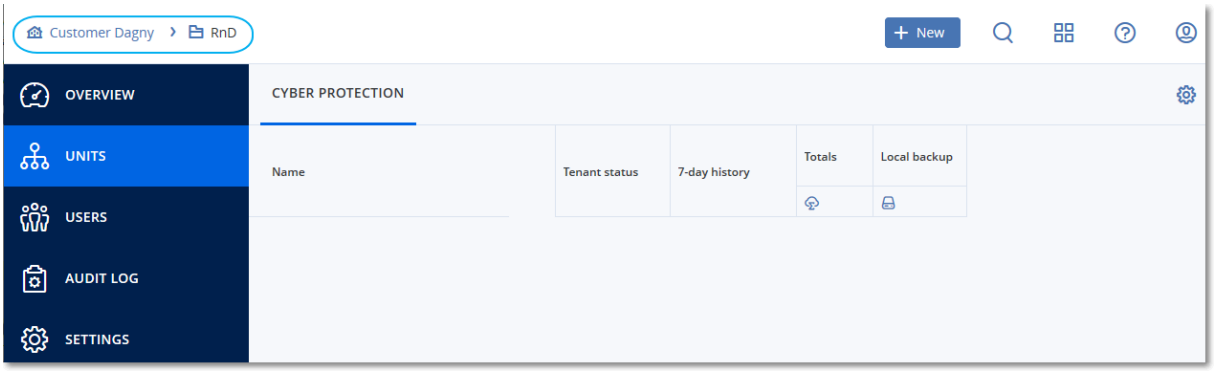
Passer du portail de gestion aux consoles de service, et vice-versa

Pour passer du portail de gestion aux consoles de service, et vice-versa, cliquez sur l'icône dans l'angle supérieur droit, puis sélectionnez **Portail de gestion** ou le service auquel vous souhaitez accéder.

Navigation dans le portail de gestion

Lorsque vous utilisez le portail de gestion, vous travaillez au sein de la société ou d'une unité à tout moment. Ceci est indiqué dans le coin supérieur gauche.

Le niveau de hiérarchie le plus haut possible est sélectionné par défaut. Cliquez sur le nom de l'unité pour explorer la hiérarchie. Pour revenir à un niveau supérieur, cliquez sur son nom dans le coin supérieur gauche.



Toutes les parties de l'interface utilisateur s'affichent et affectent uniquement la société ou l'unité dans laquelle vous travaillez actuellement. Par exemple :

- En utilisant le bouton **Nouveau**, vous pouvez créer une unité ou un compte utilisateur uniquement dans cette société ou unité.
- L'onglet **Unités** affiche uniquement les unités qui sont des enfants directs de cette société ou unité.
- L'onglet **Utilisateurs** affiche uniquement les comptes client existant dans cette société ou unité.

Création d'une unité

Ignorez cette étape si vous ne souhaitez pas organiser de comptes en unités.

Si vous prévoyez de créer des unités ultérieurement, veuillez noter que les comptes existants ne peuvent pas être déplacés entre les unités ou entre la société et les unités. Vous devez d'abord créer une unité, puis la remplir de comptes.

Pour créer une unité

1. Connectez-vous au portail de gestion.
2. Naviguez vers l'unité dans laquelle vous souhaitez créer une unité.
3. Dans l'angle supérieur droit, cliquez sur **Nouveau** > **Unité**.
4. Dans la section **Nom**, indiquez le nom de la nouvelle unité.
5. [Facultatif] Dans **Langue**, changez la langue par défaut des notifications, des rapports et du logiciel qui sera utilisée au sein de cette unité.
6. Effectuez l'une des actions suivantes :
   - Pour créer un administrateur d'unité, cliquez sur **Suivant**, puis suivez les étapes décrites dans « Création d'un compte utilisateur » à partir de l'étape 4.
   - Pour créer une unité sans administrateur, cliquez sur **Enregistrer et fermer**. Vous pourrez ajouter des administrateurs et des utilisateurs à l'unité ultérieurement.

L'unité nouvellement créée s'affiche dans l'onglet **Unités**.

Si vous souhaitez modifier les paramètres de l'unité ou indiquer des coordonnées, sélectionnez l'unité dans l'onglet **Unités**, puis cliquez sur l'icône en forme de crayon dans la section que vous souhaitez modifier.

Création d'un compte utilisateur

Ignorez cette étape si vous ne souhaitez pas créer de comptes utilisateur supplémentaires.

Vous pouvez créer des comptes supplémentaires dans les cas suivants :

- Comptes administrateur d'entreprise — pour partager les fonctions de gestion avec d'autres personnes.
- Comptes administrateur unité — pour déléguer la gestion à d'autres personnes dont les droits d'accès seront strictement limités aux unités correspondantes.
- Comptes utilisateur — pour autoriser les utilisateurs à accéder uniquement à un sous-ensemble des services.

Pour créer un compte utilisateur

1. Connectez-vous au portail de gestion.
2. Naviguez vers l'unité dans laquelle vous souhaitez créer un compte utilisateur.
3. Dans l'angle supérieur droit, cliquez sur **Nouveau** > **Utilisateur**.
4. Indiquez les informations suivantes relatives au compte :

- **Connexion**

  Important
  Chaque compte doit disposer d'un identifiant unique.

- **E-mail**

  Important
  Si l'utilisateur est enregistré dans le service File Sync & Share, indiquez l'adresse e-mail qui a été utilisée pour l'inscription File Sync & Share.
  Veuillez noter que chaque compte utilisateur du client doit disposer d'une adresse e-mail unique.

- [Facultatif] **Prénom**
- [Facultatif] **Nom**
- Dans **Langue**, changez la langue par défaut des notifications, des rapports et du logiciel qui sera utilisée pour ce compte.

5. Sélectionnez les services auxquels l'utilisateur aura accès ainsi que les rôles dans chaque service.
   - Si vous sélectionnez la case **Administrateur d'entreprise**, l'utilisateur aura accès au portail de gestion et au rôle d'administrateur dans tous les services.
   - Si vous sélectionnez la case **Administrateur d'unité**, l'utilisateur aura accès au portail de gestion, mais n'aura pas forcément le rôle d'administrateur de service, selon le service.
   - Autrement, l'utilisateur se verra attribuer les rôles que vous choisirez dans les services que vous choisirez.
6. Cliquez sur **Créer**.

Le compte utilisateur nouvellement créé s'affiche dans l'onglet **Utilisateurs**.

Si vous souhaitez modifier les paramètres utilisateur ou indiquer des paramètres de notification et des quotas pour l'utilisateur, sélectionnez l'utilisateur dans l'onglet **Utilisateurs**, puis cliquez sur l'icône en forme de crayon dans la section que vous souhaitez modifier.

Réinitialiser le mot de passe d'un utilisateur

1. Dans le portail de gestion, accédez à **Gestion d'entreprise** > **Utilisateurs**.
2. Sélectionnez l'utilisateur dont vous souhaitez réinitialiser le mot de passe, puis cliquez sur l'icône en forme de points de suspension > **Réinitialiser le mot de passe**.
3. Confirmez votre action en cliquant sur **Réinitialiser**.

L'utilisateur peut désormais suivre le processus de réinitialisation à l'aide des instructions contenues dans l'e-mail qui lui a été envoyé.

Pour les services qui ne prennent pas en charge l'authentification à deux facteurs (par exemple, l'inscription dans Cyber Infrastructure), vous devrez peut-être convertir un compte utilisateur en *compte de service*, c'est-à-dire en un compte qui ne nécessite pas d'authentification à deux facteurs.

Pour convertir un compte utilisateur dans le type du compte de service

1. Dans le portail de gestion, accédez à **Gestion d'entreprise** > **Utilisateurs**.
2. Sélectionnez l'utilisateur dont vous souhaitez convertir le compte dans le type du compte de service, puis cliquez sur l'icône en forme de points de suspension > **Marquer comme compte de service**.
3. Dans la fenêtre de confirmation, saisissez le code de l'authentification à deux facteurs et confirmez votre action.

Le compte peut désormais être utilisé pour les services qui ne prennent pas en charge l'authentification à deux facteurs.

Rôles utilisateur disponibles pour chaque service

Un utilisateur peut détenir plusieurs rôles, mais un seul par service.

Pour chaque service, vous pouvez définir quel rôle sera attribué à un utilisateur.

Service	Rôle	Description
N/D	Administrateur d'entreprise	Ce rôle accorde des droits d'administrateur complets pour tous les services. Ce rôle donne accès à la liste d'autorisation de l'entreprise. Si la fonctionnalité de reprise d'activité après sinistre du service Protection est activée pour l'entreprise, ce rôle donne également accès à la fonctionnalité de reprise d'activité après sinistre.
Portail de gestion	Administrateur	Ce rôle donne accès au portail de gestion, où l'administrateur peut gérer les utilisateurs dans l'ensemble de l'organisation. Par exemple, ce rôle attribue des autorisations complètes pour les écrans de protection évolutive des points de terminaison, y compris les widgets.
	Administrateur en lecture seule Niveau partenaire	Ce rôle fournit un accès en lecture seule à tous les objets dans le portail de gestion du partenaire et les portails de gestion de tous les clients de ce partenaire. Ces utilisateurs peuvent accéder aux données des autres utilisateurs de l'organisation en mode lecture seule. Ils peuvent modifier les plans de protection, mais ne peuvent pas enregistrer les modifications apportées aux plans de script, de surveillance ou d'agent.
	Administrateur en lecture seule	Ce rôle fournit un accès en lecture seule à tous les objets du portail de gestion de toute l'entreprise. Ces utilisateurs

	Niveau client	peuvent accéder aux données des autres utilisateurs de l'organisation en mode lecture seule.
	Administrateur en lecture seule Niveau unité	Ce rôle fournit un accès en lecture seule à tous les objets du portail de gestion de l'unité et des sous-unités de l'entreprise. Ces utilisateurs peuvent accéder aux données des autres utilisateurs de l'organisation en mode lecture seule.
Protection	Cyberadministrateur	En plus d'accorder des droits d'administrateur, ce rôle permet la configuration et la gestion du service Cyber Protection, ainsi que l'approbation d'actions dans la création de cyber-scripts. Le rôle Cyberadministrateur n'est disponible que pour les tenants pour lesquels le pack Advanced Management est activé.
	Administrateur	Ce rôle active la configuration et la gestion de Protection pour vos clients. Par exemple, ce rôle est nécessaire pour la configuration et la gestion de la fonctionnalité de reprise d'activité après sinistre, la fonctionnalité de protection évolutive des points de terminaison, ainsi que la liste d'autorisation de l'entreprise.
	Administrateur en lecture seule	Ce rôle fournit un accès en lecture seule à tous les objets du service Protection. Ces utilisateurs peuvent accéder aux données des autres utilisateurs de l'organisation en mode lecture seule. L'administrateur en lecture seule ne peut ni configurer ni gérer la fonctionnalité de reprise d'activité après sinistre, la fonctionnalité de protection évolutive des points de terminaison ou la liste d'autorisation de l'entreprise.
	Opérateur de restauration	Le rôle donne accès aux sauvegardes des organisations Microsoft 365 et Google Workspace et permet leur restauration, tout en limitant l'accès au contenu sensible.
	Utilisateur	Ce rôle permet d'utiliser le service Protection, mais sans droits d'accès d'administrateur. L'accès est fourni à la fonctionnalité telle que la protection évolutive des points de terminaison, mais les utilisateurs attribués à ce rôle ne peuvent pas accéder aux données d'autres utilisateurs dans l'organisation.
File Sync & Share	Administrateur	Ce rôle permet la configuration et la gestion de File Sync & Share pour vos utilisateurs. Un compte avec ce rôle n'est pas compté dans le quota **Utilisateurs**, car il ne fournit pas

		l'accès à la fonctionnalité File Sync & Share.
	Utilisateur	Ce rôle permet d'utiliser le service File Sync & Share. Les utilisateurs ne peuvent accéder qu'à leurs propres données et aux données qui sont partagées avec eux.
	Invité	Un compte avec ce rôle est créé lorsqu'un utilisateur de File Sync & Share partage du contenu soit avec un utilisateur de Cyber Protect Cloud qui n'a pas l'autorisation d'utiliser le service File Sync & Share, soit avec une personne qui n'est pas un utilisateur de Cyber Protect Cloud. Un rôle d'invité ne possède pas de dossier de synchronisation, ne peut pas consommer de stockage dans le cloud et n'est pas compté dans le quota **Utilisateurs**, car il ne fournit pas l'accès à la fonctionnalité File Sync & Share. Un invité ne peut pas être « promu » utilisateur ou administrateur.
Notary	Administrateur	Ce rôle permet de configurer et de gérer Notary pour vos utilisateurs.
	Utilisateur	Ce rôle permet d'utiliser le service Notary, mais sans droits d'accès d'administrateur. Ces utilisateurs ne peuvent pas accéder aux données des autres utilisateurs de l'organisation.

Rôle d'administrateur en lecture seule

Un compte avec ce rôle bénéficie d'un accès en lecture seule à la console Cyber Protect et peut effectuer les opérations suivantes :

- Collecter des données de diagnostic, comme les rapports système.
- Voir les points de récupération d'une sauvegarde, mais pas explorer le contenu de la sauvegarde ni voir les fichiers, dossiers ou e-mails.

Un administrateur en lecture seule ne peut pas effectuer les opérations suivantes :

- Démarrer ou arrêter une tâche.

  Par exemple, un administrateur en lecture seule ne peut pas démarrer une restauration ou arrêter une sauvegarde en cours d'exécution.
- Accéder au système de fichiers sur les ordinateurs source ou cible.

  Par exemple, un administrateur en lecture seule ne peut pas voir de fichiers, dossiers ou e-mails sur un ordinateur sauvegardé.
- Changer des paramètres.

  Par exemple, un administrateur en lecture seule ne peut pas créer de plan de protection ni modifier l'un de ses paramètres.

- Créer, mettre à jour ni supprimer de données.
  Par exemple, un administrateur en lecture seule ne peut pas supprimer de sauvegardes.

  Tous les objets d'interface qui ne sont pas accessibles pour un administrateur en lecture seule sont masqués, excepté les paramètres par défaut du plan de protection. Ces paramètres sont affichés, mais le bouton **Enregistrer** n'est pas actif.

  Toute modification apportée aux comptes et aux rôles s'affiche dans l'onglet **Activités**, avec les détails suivants :

  - Ce qui a été modifié
  - L'utilisateur ayant effectué la modification
  - La date et l'heure des modifications

Rôle d'opérateur de restauration

Ce rôle n'est disponible que dans le service Cyber Protection et est limité aux sauvegardes Microsoft 365 et Google Workspace.

Un opérateur de restauration peut effectuer les actions suivantes :

- Afficher les alertes et les activités
- Parcourir et actualiser la liste des sauvegardes.
- Parcourir les sauvegardes sans accéder à leur contenu. L'opérateur de restauration peut voir les noms des fichiers sauvegardés et les objets et expéditeurs des e-mails sauvegardés.
- Rechercher des sauvegardes (recherche dans le texte intégral non prise en charge).
- Restaurer des sauvegardes cloud à cloud dans leur l'emplacement d'origine au sein de l'organisation d'origine Microsoft 365 ou Google Workspace.

Un opérateur de restauration ne peut pas effectuer les actions suivantes :

- Supprimer les alertes.
- Ajouter ou supprimer des organisations Microsoft 365 ou Google Workspace.
- Ajouter, supprimer ou renommer des emplacements de sauvegarde.
- Supprimer ou renommer des sauvegardes.
- Créer, supprimer ou renommer des dossiers lors de la restauration d'une sauvegarde vers un emplacement personnalisé.
- Appliquer un plan de sauvegarde ou exécuter une sauvegarde.
- Accéder aux fichiers sauvegardés ou au contenu des e-mails sauvegardés.
- Télécharger les fichiers sauvegardés ou les pièces jointes des e-mails sauvegardés.
- Envoyer des ressources cloud sauvegardées, comme des e-mails ou des éléments de calendrier, en tant qu'e-mail.
- Afficher ou restaurer des conversations Microsoft 365 Teams.

- Restaurer des sauvegardes cloud à cloud ailleurs que dans leur emplacement d'origine, par exemple une autre boîte aux lettres, OneDrive, Google Drive ou Microsoft 365 Team.

La modification des paramètres de notification pour un utilisateur

Pour modifier les paramètres de notification d'un utilisateur, accédez à **Gestion d'entreprise** > **Utilisateurs**. Sélectionnez l'utilisateur dont vous souhaitez configurer les notifications, puis cliquez sur l'icône en forme de crayon dans la section **Paramètres**. Les paramètres de notifications suivants sont disponibles si le service Cyber Protection est activé pour le tenant dans lequel l'utilisateur est créé :

- **Notifications relatives aux dépassements de quotas** (activé par défaut)
  Les notifications relatives aux dépassements de quotas.
- **Rapports d'utilisation planifiés** (activés par défaut)
  Rapports d'utilisation envoyés le premier jour de chaque mois.
- **Notifications de labellisation d'URL** (désactivées par défaut)
  Notifications concernant l'expiration prochaine du certificat utilisé pour l'URL personnalisée des services cloud Cyber Protect. Les notifications sont envoyées à tous les administrateurs du tenant sélectionné : 30 jours, 15 jours, 7 jours, 3 jours et 1 jour avant l'expiration du certificat.
- **Notifications d'échec**, **Notifications d'avertissement** et **Notifications de réussite** (désactivées par défaut)
  Les notifications relatives aux résultats d'exécution des plans de protection et aux résultats des opérations de reprise d'activité après sinistre pour chaque terminal.
- **Résumé quotidien concernant les alertes actives** (activé par défaut)
  Le résumé quotidien est généré sur la base de la liste des alertes actives présentes dans la console Cyber Protect au moment de la génération du résumé. Le résumé est généré et envoyé une fois par jour entre 10:00 et 23:59 UTC. L'heure à laquelle le rapport est généré et envoyé dépend de la ressource du centre de données. S'il n'y a aucune alerte active, aucun résumé n'est envoyé. Le résumé n'inclut pas d'informations concernant les alertes passées qui ne sont plus actives. Par exemple, si un utilisateur trouve une sauvegarde échouée et supprime l'alerte, ou qu'il relance une sauvegarde et que celle-ci réussit avant que le résumé ne soit généré, l'alerte ne sera plus présente et le résumé ne l'affichera pas.
- **Notifications de contrôle des terminaux** (désactivées par défaut)
  Les notifications concernant les tentatives d'utilisation de périphériques et de ports restreints par des plans de protection avec le module de contrôle des terminaux activé.
- **Notifications de restauration** (désactivées par défaut)
  Les notifications concernant les actions de récupération sur les ressources suivantes : messages e-mail et boîte aux lettres complètes d'utilisateurs, dossiers publics, OneDrive / GoogleDrive : OneDrive complet et fichiers ou dossiers, Fichiers SharePoint, Teams : canaux, équipes complètes, messages e-mail et sites d'équipe.

Dans le cadre de ces notifications, les actions suivantes sont considérées comme des actions de restauration : envoi en tant qu'e-mail, téléchargement ou lancement d'une opération de récupération.

- **Notifications de prévention de perte de données** (désactivées par défaut)
  Notifications concernant les alertes de prévention de la perte de données relatives à l'activité de cet utilisateur sur le réseau.
- **Notifications d'incident de sécurité** (désactivées par défaut)
  Les notifications concernant la détection de malwares durant les analyses lors de l'accès, lors de l'exécution ou à la demande, et concernant les éléments détectés par le moteur de comportement et par le moteur de filtrage d'URL.
  Il existe deux options disponibles : **Atténué** et **Non atténué**. Ces options sont pertinentes pour les alertes d'incident de protection évolutive des points de terminaison, les alertes de protection évolutive des points de terminaison issues des flux d'informations sur les menaces et des alertes individuelles (pour les ressources dans lesquelles la protection évolutive des points de terminaison n'est pas activée).
  Lors de la création d'une alerte EDR, un e-mail est envoyé à l'utilisateur pertinent. Si le statut de la menace identifiée dans l'incident change, un nouvel e-mail est envoyé. Les e-mails comportent des boutons d'action qui permettent à l'utilisateur de voir les détails de l'incident (s'il a été atténué), ou de mener une enquête et de traiter l'incident (s'il n'a pas été atténué).
- **Notifications d'infrastructure** (désactivées par défaut)
  Notifications concernant des problèmes avec l'infrastructure de reprise d'activité après sinistre : lorsque l'infrastructure de reprise d'activité après sinistre ou les tunnels VPN ne sont pas disponibles.

Toutes les notifications sont envoyées à l'adresse e-mail de l'utilisateur.

Notifications reçues par rôle utilisateur

Les notifications envoyées par Cyber Protection dépendent du rôle utilisateur.

Types de notification\Rôle utilisateur	Utilisateur	Administrateur client
Notifications pour tous les terminaux	Oui	Oui
Notifications pour tous les terminaux de votre organisation	N/D	Oui (à l'exception des **notifications d'incident de sécurité**)
Notifications pour Microsoft 365, Google Workspace et les autres sauvegardes basées sur le Cloud	N/D	Oui

Désactivation et activation d'un compte utilisateur

Il se peut que vous deviez désactiver un compte utilisateur afin de restreindre temporairement son accès à la plate-forme Cloud.

Pour désactiver un compte utilisateur

1. Dans le portail de gestion, accédez à **Utilisateurs**.
2. Sélectionnez le compte utilisateur que vous souhaitez désactiver, puis cliquez sur l'icône en forme de points de suspension > **Désactiver**.
3. Confirmez votre action en cliquant sur **Désactiver**.

Par conséquent, cet utilisateur ne pourra plus utiliser la plate-forme Cloud ni recevoir de notifications.

Pour activer un compte utilisateur désactivé, sélectionnez-le dans la liste des utilisateurs, puis cliquez sur l'icône en forme de points de suspension > **Activer**.

Suppression d'un compte utilisateur

Il se peut que vous deviez supprimer un compte utilisateur de façon permanente afin de libérer les ressources qu'il utilise, comme de l'espace de stockage ou une licence. Les statistiques d'utilisation seront mises à jour sous un jour après suppression. En ce qui concerne les comptes contenant beaucoup de données, il se peut que ce délai soit plus long.

Avant de supprimer un compte utilisateur, vous devez le désactiver. Pour en savoir plus sur la façon de procéder, reportez-vous à « Désactivation et activation d'un compte utilisateur ».

Pour supprimer un compte utilisateur

1. Dans le portail de gestion, accédez à **Utilisateurs**.
2. Sélectionnez le compte utilisateur désactivé, puis cliquez sur l'icône en forme de points de suspension > **Supprimer**.
3. Pour confirmer votre action, saisissez votre identifiant, puis cliquez sur **Supprimer**.

En conséquence :

- Toutes les notifications configurées pour ce compte seront désactivées.
- Toutes les données appartenant à ce compte utilisateur seront supprimées.
- L'administrateur n'aura pas accès au portail de gestion.
- Toutes les sauvegardes des ressources associées à cet utilisateur seront supprimées.
- Toutes les machines associées à ce compte utilisateur seront désenregistrées.
- Tous les plans de protection seront révoqués pour toutes les ressources associées à cet utilisateur.
- Toutes les données File Sync & Share appartenant à cet utilisateur (par exemple, les fichiers et les dossiers) seront supprimées.
- Les données de Notary appartenant à cet utilisateur (par exemple, les fichiers notariés, les fichiers signés électroniquement) seront supprimées.

- L'**état** de l'utilisateur indique **Supprimé**. Lorsque vous survolez l'état **Supprimé**, la date de suppression de l'utilisateur apparaît, ainsi qu'une remarque indiquant que vous pouvez toujours restaurer tous les paramètres et données de l'utilisateur pertinents dans les 30 jours suivant la date de leur suppression.

Transférer la propriété d'un compte utilisateur

Il se peut que vous deviez transférer la propriété d'un compte utilisateur si vous souhaitez conserver l'accès aux données d'un utilisateur restreint.

Important
Vous ne pouvez pas réaffecter le contenu d'un compte supprimé.

Pour transférer la propriété d'un compte utilisateur :

1. Dans le portail de gestion, accédez à **Utilisateurs**.
2. Sélectionnez le compte utilisateur dont vous souhaitez transférer la propriété, puis cliquez sur l'icône en forme de crayon dans la section **Informations générales**.
3. Remplacez l'adresse e-mail existante par l'adresse e-mail du futur propriétaire du compte, puis cliquez sur **Terminé**.
4. Confirmez votre action en cliquant sur **Oui**.
5. Laissez le futur propriétaire du compte valider son adresse e-mail en suivant les instructions qui lui seront envoyées.
6. Sélectionnez le compte utilisateur dont vous transférez la propriété, puis cliquez sur l'icône en forme de points de suspension > **Réinitialiser le mot de passe**.
7. Confirmez votre action en cliquant sur **Réinitialiser**.
8. Laissez le futur propriétaire du compte réinitialiser le mot de passe en suivant les instructions qui lui seront envoyées par e-mail.

Le nouveau propriétaire peut désormais accéder à ce compte.

Configurer l'authentification à deux facteurs

L'authentification à deux facteurs (2FA) est un type d'authentification à plusieurs facteurs, qui vérifie l'identité d'un utilisateur en utilisant une association de deux facteurs différents :

- Un élément qu'un utilisateur connaît (un code PIN ou un mot de passe)
- Un élément qu'un utilisateur possède (un jeton)
- Un élément qui fait partie d'un utilisateur (biométrie)

L'authentification à deux facteurs vous protège davantage contre l'accès non autorisé à votre compte.

La plate-forme est compatible avec l'authentification par **mot de passe unique basée sur le temps (TOTP)** . Si l'authentification TOTP est activée dans le système, les utilisateurs doivent saisir leur mot de passe habituel ainsi que le code TOTP unique pour accéder au système. En d'autres termes, un utilisateur fournit le mot de passe (premier facteur) et le code TOTP (second facteur). Le code TOTP est généré dans l'application d'authentification du terminal qui applique le second facteur, sur la base de l'heure actuelle et du code secret (QR code ou code alphanumérique) fourni par la plateforme.

Fonctionnement

1. Vous activez l'authentification à deux facteurs au niveau de votre organisation.
2. Tous les utilisateurs de l'organisation doivent installer une application d'authentification sur le terminal qui applique le second facteur (téléphone mobile, ordinateur portable ou de bureau, ou tablette). Cette application sera utilisée pour générer des codes TOTP uniques. Les authentificateurs recommandés sont les suivants :
   - Google Authenticator
     Version de l'application iOS (https://apps.apple.com/app/google-authenticator/id388497605)
     Version Android (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2)
   - Microsoft Authenticator
     Version de l'application iOS (https://apps.apple.com/app/microsoft-authenticator/id983156458)
     Version Android (https://play.google.com/store/apps/details?id=com.azure.authenticator)

   Important
   Les utilisateurs doivent s'assurer que l'heure indiquée sur le terminal sur lequel l'application d'authentification est installée est correctement définie, et reflète bien l'heure actuelle.
3. Les utilisateurs de votre organisation doivent se reconnecter au système.
4. Après avoir saisi leur identifiant et leur mot de passe, ils seront invités à configurer l'authentification à deux facteurs pour leur compte utilisateur.
5. Ils doivent scanner le QR code en utilisant leur application d'authentification. S'il est impossible de scanner le QR code, ils peuvent utiliser le code de 32 chiffres indiqué en dessous du QR code et l'ajouter manuellement dans l'application d'authentification.

   Important
   Il est vivement recommandé de l'enregistrer (imprimez le QR code, notez le mot de passe temporaire à usage unique (TOTP), utilisez l'application prenant en charge la sauvegarde de codes dans un cloud). Vous aurez besoin du mot de passe temporaire à usage unique (TOTP) pour réinitialiser l'authentification à deux facteurs si vous perdez le terminal qui applique le second facteur.

6. Le mot de passe temporaire à usage unique (TOTP) sera généré dans l'application d'authentification. Il est automatiquement régénéré toutes les 30 secondes.
7. Dans la fenêtre **Configurer l'authentification à deux facteurs**, les utilisateurs doivent saisir le mot de passe temporaire à usage unique après avoir saisi leur mot de passe.
8. En conséquence, l'authentification à deux facteurs sera configurée pour les utilisateurs.

Désormais, lorsque les utilisateurs se connecteront au système, ils seront invités à fournir l'identifiant et le mot de passe, puis le code TOTP unique généré dans l'application d'authentification. Les utilisateurs peuvent indiquer que le navigateur est un navigateur fiable lorsqu'ils se connectent au système. Le code TOTP ne sera pas demandé lors des connexions suivantes effectuées avec ce navigateur.

Pour restaurer l'authentification à deux facteurs sur un nouveau terminal

Si vous avez accès à l'application d'authentification sur mobile configurée précédemment :

1. Installez une application d'authentification sur votre nouveau terminal.
2. Utilisez le fichier PDF que vous avez enregistré lorsque vous avez configuré l'authentification à deux facteurs sur votre terminal. Ce fichier contient le code à 32 chiffres qui doit être saisi dans l'application d'authentification pour réassocier cette application à votre compte Acronis.

   Important
   Si le code est correct, mais ne fonctionne pas, veillez à synchroniser l'heure dans l'application d'authentification pour mobile.

3. Si vous n'avez pas enregistré le fichier PDF pendant l'installation :

a. *Cliquez sur **Réinitialiser l'authentification à deux facteurs** et saisissez le mot de passe à usage unique dans l'application d'authentification sur mobile configurée précédemment.*
b. Suivez les instructions affichées à l'écran.

Si vous n'avez pas accès à l'application d'authentification sur mobile configurée précédemment :

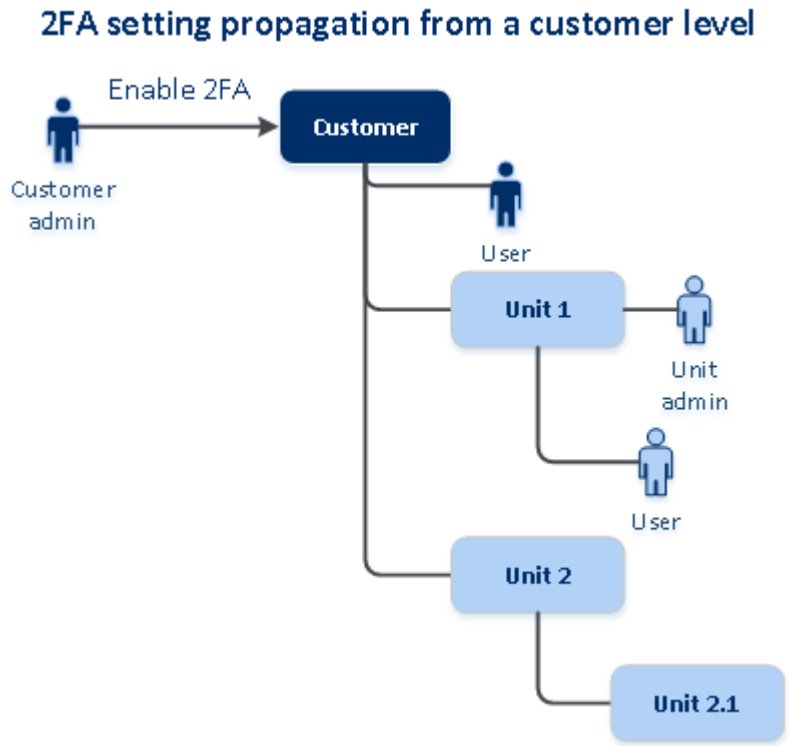
1. Prenez un nouveau terminal mobile.
2. Utilisez le fichier PDF stocké pour associer un nouveau terminal (le nom par défaut du fichier est `cyberprotect-2fa-backupcode.pdf`).
3. Restaurez l'accès à votre compte depuis la sauvegarde. Assurez-vous que les sauvegardes sont prises en charge par votre application mobile.
4. Ouvrez l'application dans le même compte, depuis un autre terminal mobile s'il est pris en charge par l'application.

Propagation de la configuration de l'authentification à deux facteurs à tous les niveaux de tenants

L'authentification à deux facteurs est définie au niveau de l'**organisation**. Vous pouvez configurer l'authentification à deux facteurs pour votre propre organisation uniquement.

Les paramètres de l'authentification à deux facteurs se propagent à tous les niveaux de tenants de la façon suivante :

- Les unités héritent automatiquement des paramètres d'authentification à deux facteurs de l'organisation cliente.



Remarque

1. Il n'est pas possible de configurer l'authentification à deux facteurs au niveau de l'unité.
2. Vous pouvez gérer les paramètres de l'authentification à deux facteurs pour les utilisateurs des organisations enfants (unités).

Configurer l'authentification à deux facteurs pour votre tenant

En tant qu'administrateur, vous pouvez activer l'authentification à deux facteurs pour votre organisation.

Pour activer l'authentification à deux facteurs pour votre tenant

1. Dans le portail de gestion, accédez à **Paramètres** > **Sécurité**.
2. Faites glisser le commutateur **Authentification à deux facteurs**, puis cliquez sur **Activer**.

À présent, tous les utilisateurs dans l'organisation doivent configurer l'authentification à deux facteurs pour leur compte. Ils seront invités à le faire la prochaine fois qu'ils essaieront de se connecter ou lors de l'expiration de leur session actuelle.

La barre de progression sous le commutateur affiche le nombre d'utilisateurs ayant configuré l'authentification à deux facteurs pour leur compte. Pour vérifier quels utilisateurs ont configuré leur compte, accédez à **Gestion d'entreprise** > onglet **Utilisateurs**, puis consultez la colonne **Statut 2FA**. Le statut 2FA (authentification à deux facteurs) des utilisateurs qui n'ont pas encore configuré ce type d'authentification pour leur compte est **Configuration requise**.

Une fois la configuration de l'authentification à deux facteurs réussie, les utilisateurs devront saisir leur identifiant, leur mot de passe et un code TOTP à chaque connexion à la console de service.

Pour désactiver l'authentification à deux facteurs pour votre tenant

1. Dans le portail de gestion, accédez à **Paramètres** > **Sécurité**.
2. Pour désactiver l'authentification à deux facteurs, désactivez le commutateur, puis cliquez sur **Désactiver**.
3. [Si au moins un utilisateur au sein de l'organisation a configuré l'authentification à deux facteurs] Saisissez le code TOTP généré dans l'application d'authentification de votre terminal mobile.

En conséquence, l'authentification à deux facteurs est désactivée pour votre organisation, tous les secrets sont supprimés et tous les navigateurs fiables sont oubliés. Tous les utilisateurs se connecteront au système en utilisant uniquement leur identifiant et leur mot de passe. Dans **Gestion d'entreprise** > onglet **Utilisateurs**, la colonne **Statut 2FA** est masquée.

Gestion de l'authentification à 2 facteurs pour les utilisateurs

Vous pouvez surveiller les paramètres d'authentification à deux facteurs de tous vos utilisateurs et réinitialiser les paramètres dans le portail de gestion, dans **Gestion d'entreprise** > **Utilisateurs**.

Surveillance

Dans le portail de gestion, sous **Gestion d'entreprise** > **Utilisateurs**, vous pouvez voir la liste de tous les utilisateurs de votre organisation. Le **statut 2FA** indique si l'authentification à deux facteurs est configurée pour un utilisateur.

Pour réinitialiser l'authentification à deux facteurs pour un utilisateur

1. Dans le portail de gestion, accédez à **Gestion d'entreprise** > **Utilisateurs**.
2. Dans l'onglet **Utilisateurs**, recherchez un utilisateur dont vous souhaitez modifier les paramètres, puis cliquez sur l'icône en forme de points de suspension.
3. Cliquez sur **Réinitialiser l'authentification à deux facteurs**.
4. Saisissez le code TOTP généré dans l'application d'authentification du terminal qui applique le second facteur, puis cliquez sur **Réinitialiser**.

En conséquence, l'utilisateur pourra de nouveau configurer l'authentification à deux facteurs.

Pour réinitialiser les navigateurs fiables pour un utilisateur

1. Dans le portail de gestion, accédez à **Gestion d'entreprise** > **Utilisateurs**.
2. Dans l'onglet **Utilisateurs**, recherchez un utilisateur dont vous souhaitez modifier les paramètres, puis cliquez sur l'icône en forme de points de suspension.
3. Cliquez sur **Réinitialiser tous les navigateurs fiables**.
4. Saisissez le code TOTP généré dans l'application d'authentification du terminal qui applique le second facteur, puis cliquez sur **Réinitialiser**.

L'utilisateur pour qui vous avez réinitialisé tous les navigateurs fiables devra fournir le code TOTP lors de sa prochaine connexion.

Les utilisateurs peuvent eux-mêmes réinitialiser tous les navigateurs fiables, ainsi que les paramètres d'authentification à deux facteurs. Cette opération peut être effectuée lorsqu'ils se connectent au système, en cliquant sur le lien respectif et en saisissant le code TOTP pour confirmer l'opération.

Pour désactiver l'authentification à deux facteurs pour un utilisateur

Nous ne recommandons pas de désactiver l'authentification à deux facteurs parce que cela peut créer des brèches dans la sécurité des tenants.

À titre d'exception, vous pouvez désactiver l'authentification à deux facteurs pour un utilisateur et la conserver pour tous les autres utilisateurs du tenant. C'est une solution de contournement pour les cas où l'authentification à deux facteurs est activée au sein d'un tenant où une configuration cloud est configurée, et où cette intégration s'authentifie sur la plate-forme via le compte utilisateur (identifiant et mot de passe). Pour poursuivre l'utilisation de l'intégration en tant que solution temporaire, il est possible de transformer l'utilisateur en un compte de service auquel l'authentification à deux facteurs n'est pas applicable.

Important
La transformation d'utilisateurs standard en utilisateurs de service afin de désactiver l'authentification à deux facteurs n'est pas recommandée parce qu'elle est risquée pour la sécurité des tenants.

La solution sûre et recommandée pour l'utilisation d'intégrations cloud sans désactivation de l'authentification à deux facteurs pour les tenants consiste à créer des clients API et à configurer vos intégrations cloud de manière à ce qu'elles fonctionnent de concert.

1. Dans le portail de gestion, accédez à **Gestion d'entreprise** > **Utilisateurs**.
2. Dans l'onglet **Utilisateurs**, recherchez un utilisateur dont vous souhaitez modifier les paramètres, puis cliquez sur l'icône en forme de points de suspension.
3. Cliquez sur **Marquer comme compte de service**. En conséquence, un utilisateur reçoit un statut spécial d'authentification à deux facteurs, appelé **Compte de service.**

4. [Si au moins un utilisateur au sein d'un tenant a configuré l'authentification à deux facteurs] Pour confirmer la désactivation, saisissez le code TOTP généré dans l'application d'authentification du terminal qui applique le second facteur.

Pour activer l'authentification à deux facteurs pour un utilisateur

Vous devrez peut-être activer l'authentification à deux facteurs pour un utilisateur en particulier, pour qui vous l'aviez auparavant désactivée.

1. Dans le portail de gestion, accédez à **Gestion d'entreprise** > **Utilisateurs**.
2. Dans l'onglet **Utilisateurs**, recherchez un utilisateur dont vous souhaitez modifier les paramètres, puis cliquez sur l'icône en forme de points de suspension.
3. Cliquez sur **Marquer comme compte normal**. En conséquence, un utilisateur devra configurer l'authentification à deux facteurs ou fournir le code TOTP lorsqu'il accèdera au système.

Réinitialisation de l'authentification à deux facteurs en cas de perte du terminal qui applique le second facteur

Pour réinitialiser l'accès à votre compte en cas de perte du terminal qui applique le second facteur, suivez l'une des approches suggérées :

- Restaurez votre code secret TOTP (QR code ou code alphanumérique) depuis une sauvegarde. Utilisez un autre terminal appliquant le second facteur et ajoutez le code secret TOTP dans l'application d'authentification installé sur ce terminal.
- Demandez à votre administrateur de réinitialiser les paramètres de l'authentification à deux facteurs pour vous.

Protection contre les attaques en force brute

Une attaque en force brute est une attaque au cours de laquelle un intrus tente d'accéder au système en soumettant plusieurs mots de passe, dans l'espoir que l'un de ces mots de passe soit correct.

Le mécanisme de protection contre les attaques en force brute de la plateforme est basé sur les cookies de périphérique.

Les paramètres de protection contre les attaques en force brute qui sont utilisés sur la plateforme sont prédéfinis :

Paramètre	Saisie du mot de passe	Saisie du code TOTP
Limite de tentatives	10	5
Période de la limite de tentatives (la limite est réinitialisée une fois le délai expiré)	15 min (900 s)	15 min (900 s)

Le verrouillage a lieu au	Limite de tentatives + 1 (11e tentative)	Limite de tentatives
Période de verrouillage	5 min (300 s)	5 min (300 s)

Si vous avez activé l'authentification à deux facteurs, un cookie de terminal est envoyé au client (navigateur) uniquement après que l'authentification ait réussi à l'aide des deux facteurs (mot de passe et code TOTP).

Pour les navigateurs fiables, le cookie de terminal est envoyé après que l'authentification ait réussi uniquement à l'aide d'un facteur (mot de passe).

Les tentatives de saisie de code TOTP sont enregistrées pour chaque utilisateur, et non pour chaque terminal. Cela signifie que si un utilisateur tente de saisir le code TOTP à l'aide de différents terminaux, il sera bloqué.

Mise à jour automatique des agents

Important
Actuellement, vous n'avez accès à la fonctionnalité de gestion de mise à jour des agents que si vous avez activé Protection.

Cyber Protect possède trois types d'agents qui peuvent être installés sur des machines protégées : Agent pour Windows, agent pour Linux et agent pour Mac.

Cloud Cyber Files possède une version de l'agent de bureau File Sync & Share pour Windows et une autre pour macOS, qui permet la synchronisation de fichiers et de dossiers entre un ordinateur et la zone de stockage dans le cloud File Sync & Share d'un utilisateur afin de promouvoir le travail hors ligne, ainsi que le télétravail et les pratiques BYOD (Bring Your Own Device - Apporter votre propre terminal).

Pour faciliter la gestion de plusieurs ressources, vous pouvez configurer (et désactiver) les mises à jour automatiques et sans assistance pour tous les agents sur tous les ordinateurs.

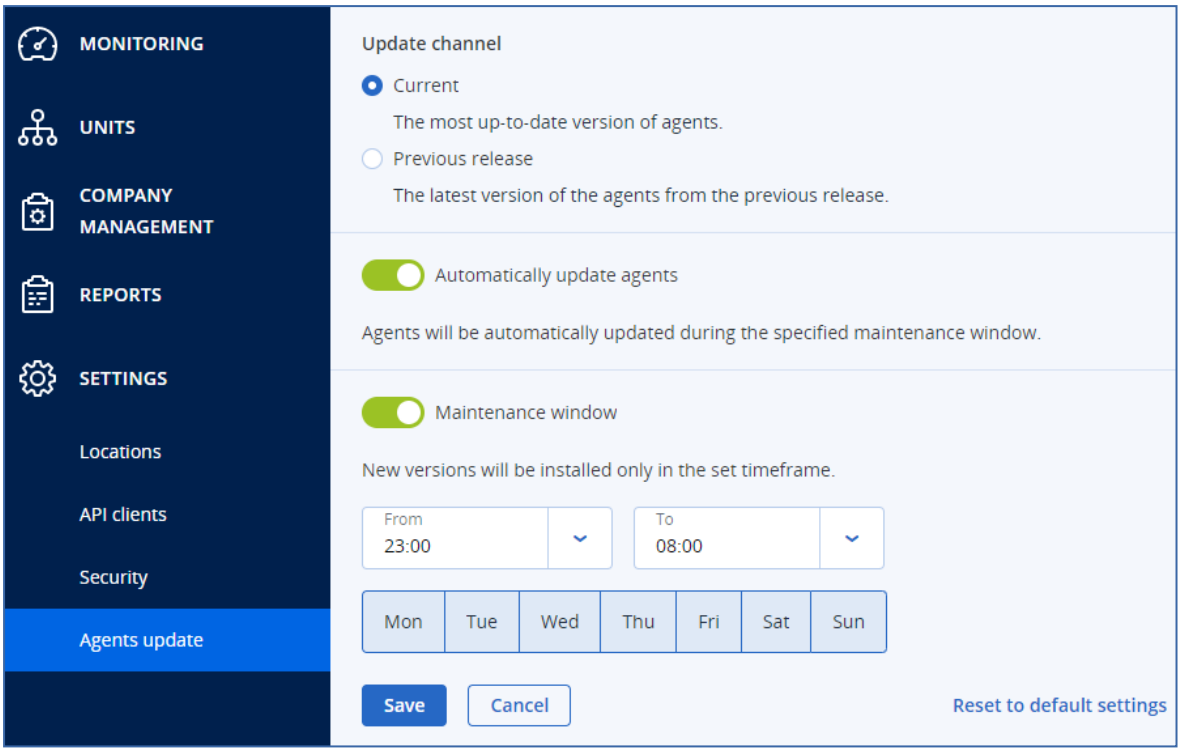
Remarque
Pour gérer les agents sur des machines individuelles, et personnaliser les paramètres de mise à jour automatique, veuillez consulter la section du Guide de l'utilisateur Cyber Protect consacrée à la Mise à jour des agents.

Mettre à jour automatiquement des agents

Remarque
Les paramètres de mise à jour automatique de l'agent pour File Sync & Share sont hérités de votre fournisseur de services si vous n'avez pas activé le module Protection.

Configurer une mise à jour automatique des agents depuis la page initiale du portail de gestion

1. Cliquez sur **Paramètres > Mise à jour des agents**.



2. Sélectionnez la version à détecter pour les mises à jour automatiques : **Actuelle** ou **Version précédente**.
   (la valeur par défaut est **Actuelle**.)
3. Activez l'option **Mettre à jour automatiquement les agents**.
   (L'option est **activée** par défaut.)
4. Définissez la fenêtre de maintenance.
   (La fenêtre de maintenance par défaut est 23 h à 08 h.)

Remarque
Bien que les processus de mise à jour des agents soient conçus pour être rapides et transparents, nous vous recommandons de choisir une fenêtre qui engendrera le moins de perturbation pour les utilisateurs. En effet, les utilisateurs ne peuvent pas empêcher ni reporter les mises à jour automatiques.

5. [Facultatif] Sélectionnez les jours lors desquels effectuer les mises à jour.
6. Sélectionnez **Enregistrer.**

Remarque
Les mises à jour automatiques sont uniquement disponibles pour :

- Les agents Cyber Protect version 15.0.26986 (publiée en mai 2021) et versions ultérieures.
- L'agent de bureau File Sync & Share version 15.0.30370 et versions ultérieures.

Pour les agents plus anciens, vous devez d'abord effectuer une mise à jour à la dernière version avant que les mises à jour automatiques puissent prendre effet.

Surveiller les mises à jour des agents

Important
Les mises à jour des agents ne peuvent être surveillées que si vous avez activé le module Protection.

Pour surveiller les mises à jour des agents, veuillez consulter les sections Alertes et Activités du Guide de l'utilisateur Cyber Protect.

Configuration d'un stockage immuable

Grâce au stockage immuable, vous pouvez accéder à des sauvegardes supprimées pendant une période de rétention spécifiée. Vous pouvez restaurer du contenu depuis ces sauvegardes, mais vous ne pouvez ni les modifier, ni les déplacer, ni les supprimer. À la fin de la période de rétention, les sauvegardes supprimées sont définitivement supprimées.

Le stockage immuable contient les sauvegardes suivantes :

- Sauvegardes supprimées manuellement.
- Sauvegardes supprimées automatiquement, conformément aux paramètres de la section **Durée de conservation** d'un plan de protection ou de la section **Règles de rétention** d'un plan de nettoyage.

Les sauvegardes supprimées du stockage immuable utilisent toujours de l'espace de stockage et sont facturées en conséquence.

Les tenants supprimés ne sont facturés pour aucun stockage, pas même le stockage immuable.

Pour les tenants de clients, le stockage immuable est disponible dans les modes suivants :

- **Mode de gouvernance**
  Vous pouvez désactiver et réactiver le stockage immuable. Vous pouvez modifier la période de rétention ou passer en mode de conformité.
- **Mode de conformité**

  Avertissement !
  La sélection du mode de conformité est irréversible.

Vous ne pouvez pas désactiver le stockage immuable. Vous ne pouvez pas modifier la période de rétention ni revenir au mode de gouvernance.

La configuration des paramètres de stockage immuable exige l'authentification à deux facteurs dans le tenant à qui le compte administrateur appartient.

Remarque
Pour permettre l'accès aux sauvegardes supprimées, le port 40440 sur le stockage des sauvegardes doit être activé pour les connexions entrantes.

Pour activer le stockage immuable

1. Connectez-vous au portail de gestion en tant qu'administrateur, puis accédez à **Paramètres** > **Sécurité**.
2. Activez le commutateur **Stockage immuable**.
3. Spécifiez une période de rétention comprise entre 14 et 3 650 jours.
   Par défaut, la période de rétention est de 14 jours. Une période de rétention plus longue augmentera l'utilisation du stockage.
4. Sélectionnez le mode de stockage immuable et, si le système vous y invite, confirmez votre choix.
5. Cliquez sur **Enregistrer**.

   Avertissement !
   La sélection du **Mode de conformité** est irréversible. Après avoir sélectionné ce mode, vous ne serez plus autorisé à désactiver le stockage immuable, ni à modifier son mode ou sa période de rétention.

6. Pour qu'une archive existante prenne en charge le stockage immuable, créez une nouvelle sauvegarde dans cette archive.
   Pour créer une nouvelle sauvegarde, exécutez le plan de protection manuellement ou selon une planification.

   Avertissement !
   Si vous supprimez une sauvegarde avant de configurer l'archive pour qu'elle prenne en charge le stockage immuable, la sauvegarde sera supprimée définitivement.

Pour désactiver le stockage immuable

1. Connectez-vous au portail de gestion en tant qu'administrateur, puis accédez à **Paramètres** > **Sécurité**.
2. Désactivez le commutateur **Stockage immuable**.

   Remarque
   Vous pouvez désactiver le stockage immuable uniquement en mode de gouvernance.

Avertissement !
La désactivation du stockage immuable n'entre pas en vigueur immédiatement. Pendant une période de grâce de 14 jours, le stockage immuable reste actif et vous pouvez accéder aux sauvegardes supprimées pendant leur période de rétention d'origine. À la fin de la période de grâce, toutes les sauvegardes stockées dans le stockage immuable sont définitivement supprimées.

3. Confirmez votre choix en cliquant sur **Désactiver**.

Stockages et agents pris en charge

- Le stockage immuable n'est pris en charge que pour le stockage dans le cloud.
  Le stockage immuable est disponible pour les stockages dans le cloud hébergés par Acronis et ses partenaires qui utilisent Cyber Infrastructure version 4.7.1 ou ultérieure.
  Tous les systèmes de stockage pouvant être utilisés avec Cyber Infrastructure Backup Gateway sont pris en charge. Par exemple, le stockage Cyber Infrastructure, les stockages Amazon S3 et EC2, et le stockage Microsoft Azure.
  Le stockage immuable nécessite que le port TCP 40440 soit ouvert pour le service Backup Gateway dans Cyber Infrastructure. Dans les versions 4.7.1 et ultérieure, le port TCP 40440 est automatiquement ouvert avec le type de trafic **public Backup (ABGW)**. Pour plus d'informations sur les types de trafic, consultez la documentation d'Acronis Cyber Infrastructure.
- Le stockage immuable nécessite un agent de protection version 21.12 (15.0.28532) ou ultérieure.
- Seules les sauvegardes TIBX (version 12) sont prises en charge.

Gestion des tâches

Si votre compte comprend l'accès au service Advanced Automation, cliquez sur **Gestion des tâches** pour afficher et gérer vos tickets auprès du service d'assistance.

Remarque
Les utilisateurs auxquels le rôle Gestionnaire des clients a été attribué dans Advanced Automation peuvent voir et gérer tous les tickets du service d'assistance dans l'organisation ; ceux ayant le rôle Client ne peuvent voir et mettre à jour que leurs propres tickets.

Affichage des tickets auprès du service d'assistance

Pour afficher les tickets existants du service d'assistance, accédez depuis le portail de gestion à **Gestion des tâches > Service d'assistance**. Les informations concernant chaque ticket sont affichées :

- Lien vers le ticket.
- Statut actuel du ticket.
- Total du temps passé sur le ticket.
- Utilisateur ayant fait la demande de ticket.
- Client.
- Priorité du ticket.
- Agent du support affecté.
- Accord de niveau de service (SLA) attribué, moment de violation de cet accord et prochaine mise à jour prévue de la part d'un ingénieur dédié.
- Date de dernière mise à jour du ticket.

Pour exporter des données de tickets, cliquez sur **Exporter**. Un fichier XLS intitulé **Tickets** est téléchargé sur votre ressource.

Vous pouvez également filtrer et trier la liste qui s'affiche pour retrouver un ticket spécifique ; si vous souhaitez un filtrage plus précis, utilisez l'outil **Filtrer** pour définir les tickets à afficher.

Création d'un ticket auprès du service d'assistance

Pour créer un nouveau ticket

1. Accédez à **Gestion des tâches > Service d'assistance**. La liste des tickets ouverts s'affiche.

   Remarque
   Les utilisateurs auxquels le rôle Gestionnaire des clients a été attribué dans Advanced Automation voient tous les tickets du service d'assistance dans l'organisation ; ceux ayant le rôle Client ne voient que leurs propres tickets.

2. Cliquez sur **+ Nouveau**. La boîte de dialogue Créer un nouveau ticket s'affiche.
3. Définissez ce qui suit :
   - Dans le champ **Titre du ticket**, ajoutez le titre du ticket.
   - Dans le champ **Demandeur** (activé uniquement pour les utilisateurs ayant le rôle Gestionnaire des clients), sélectionnez l'utilisateur souhaité dans la liste des contacts et utilisateurs actifs du client. Notez que le champ **Nom du client** est désactivé pour les utilisateurs Gestionnaire des clients et Client.
   - (Facultatif) Dans le champ **Numéro de téléphone**, ajoutez un numéro de téléphone. Notez que, si vous mettez à jour le numéro par défaut, le nouveau numéro est stocké en tant que numéro de téléphone par défaut de l'utilisateur.
   - Dans le champ **Supérieur**, sélectionnez l'utilisateur souhaité dans la liste des utilisateurs actifs du client (par exemple, les utilisateurs auxquels le rôle Gestionnaire des clients est affecté).
   - Dans la section **Élément ou service de configuration**, sélectionnez un **service géré** ou un **service informatique** :
     - **Service géré** : Cette option est sélectionnée et préremplie avec les détails nécessaires si le type de produit Service géré est disponible dans le contrat pertinent. Notez que, si le contrat ne comporte aucun type de produit de service géré, cette option est désactivée.
     - **Service informatique** : Cette option est sélectionnée et préremplie avec les détails nécessaires si le type de produit Service informatique est disponible dans le contrat pertinent. Notez que, si le contrat ne comporte aucun type de produit de service informatique, cette option est désactivée.
     - Le champ **Élément de configuration** indique les terminaux associés au service géré ou informatique sélectionné (le message **Élément de configuration inconnu** est affiché si le terminal est inconnu) ; la sélection d'un terminal après celle d'un service est facultative (lorsque vous sélectionnez un terminal dans ce scénario, l'accord de niveau de service (SLA) ne change pas ; il reste l'accord de niveau de service (SLA) qui appartient au service).

       Remarque
       Les terminaux répertoriés comprennent ceux fournis par Cyber Protect. Si Cyber Protection fournit une option de contrôle distant pour un terminal répertorié, vous pouvez vous connecter à distance depuis le ticket à l'aide du protocole RDP ou d'un client HTML5.

     - Vous pouvez également sélectionner une catégorie dans le champ **Catégorie**, puis définir une priorité dans le champ **Priorité**. Le champ **Accord de niveau de service (SLA)** indique l'accord de niveau de service (SLA) passé avec votre fournisseur de services managés.

- Dans la section **Mise à jour du ticket**, vous pouvez ajouter des descriptions et commentaires en texte enrichi (y compris des images et d'autres fichiers média pour un maximum de 25 Mo ; les formats et types pris en charge sont répertoriés ci-dessous dans la section **Pièces jointes**) de la zone de texte. Notez que le statut du ticket est défini par défaut sur **Nouveau** et qu'il ne peut pas être modifié.
- Cliquez pour activer le bouton bascule **Envoyer un e-mail au demandeur** afin que les mises à jour de ticket soient envoyées par e-mail au demandeur.
- Dans la section **Pièces jointes**, cliquez sur les pièces jointes nécessaires (ou utilisez le glisser-déposer) pour les ajouter.

  Les pièces jointes peuvent inclure les formats et types suivants (jusqu'à un maximum de 25 Mo) :
  - Média : .avi, .mp4, .mp3
  - E-mails : .eml, .msg
  - Images : .png, .gif, .jpeg, .jpg, .heic, .bmp, .tiff, .svg
  - Fichiers de document et de journal : .doc, .docx, .xls, .xlsx, .ppt, .pptx, .txt, .log, .pdf
  - Archives : .zip, .rar

4. Cliquez sur **Valider**. Une fois le ticket généré, il est ajouté à la liste des tickets ouverts.

Mise à jour des tickets auprès du service d'assistance

Pour mettre à jour un ticket

1. Accédez à **Gestion des tâches > Service d'assistance**. La liste des tickets ouverts s'affiche.

   Remarque
   Les utilisateurs auxquels le rôle Gestionnaire des clients a été attribué dans Advanced Automation voient tous les tickets du service d'assistance dans l'organisation ; ceux ayant le rôle Client ne voient que leurs propres tickets.

2. (Facultatif) Si vous avez un grand nombre de tickets, utilisez le filtre pour localiser le ou les tickets que vous recherchez.

   Cliquez sur **Filtre** (ou **Filtres enregistrés** si vous avez déjà défini un filtre), puis sélectionnez les valeurs pertinentes dans les différents champs. Notez que vous pouvez cliquer sur l'option **Ajouter aux filtres enregistrés** pour enregistrer le filtre défini à des fins ultérieures.

   Vous pouvez également utiliser la barre **Recherche** pour localiser le ou les tickets pertinents.
3. Cliquez sur le lien de la ligne de ticket approprié et apportez les modifications nécessaires dans les onglets affichés :
   - **Activités** : Affiche l'activité récente sur le ticket, y compris le statut actuel et les commentaires ajoutés.

Remarque
Si vous modifiez le statut d'un ticket créé par une alerte dans la console Cyber Protect et sélectionnez **Fermé**, l'alerte est également fermée dans la console Cyber Protect.

- **Vue d'ensemble** : Affiche les paramètres généraux de ticket pouvant être modifiés ; pour plus d'informations, voir "Création d'un ticket auprès du service d'assistance" (p. 40).
  Notez que vous pouvez modifier le statut du ticket dans cet onglet. Par exemple, vous pouvez mettre à jour son statut et sélectionner **En progrès** lorsque vous commencez à travailler sur ce ticket ou **Fermé** lorsque le ticket peut être clos. Vous pouvez également modifier les terminaux associés à un ticket ; par exemple, si un ticket créé n'indique pas le terminal correct, vous pouvez cliquer sur la liste déroulante **Élément de configuration** pour sélectionner le terminal adéquat.

Pour plus d'informations sur les différents champs disponibles lors de la modification d'un ticket, voir "Création d'un ticket auprès du service d'assistance" (p. 40).

4. Cliquez sur **Enregistrer les modifications**.
   Notez que, si le bouton bascule **Envoyer un e-mail au demandeur** est activé, un e-mail est envoyé à l'utilisateur pertinent.

Surveillance

Pour accéder aux informations relatives à l'utilisation des services et aux opérations, cliquez sur **Surveillance**.

Utilisation

L'onglet **Utilisation** fournit une vue d'ensemble de l'utilisation du service (notamment les quotas éventuels) et vous permet d'accéder aux consoles de service.

Pour actualiser les données d'utilisation qui s'affichent dans l'onglet, cliquez sur les points de suspension en haut à droite de l'écran, puis sélectionnez **Actualiser l'utilisation**.

Remarque
La récupération des données peut prendre jusqu'à 10 minutes. Rechargez la page pour afficher les données mises à jour.

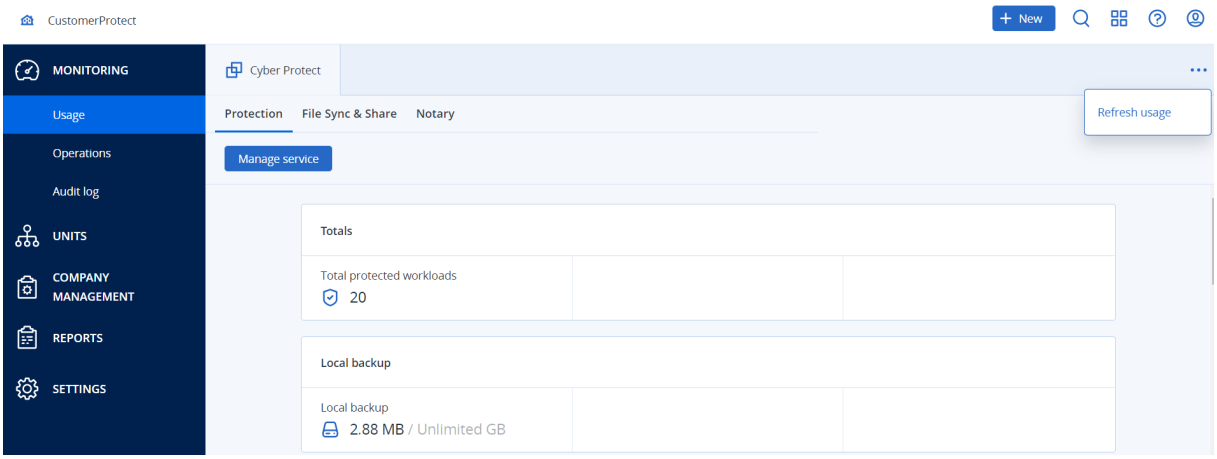


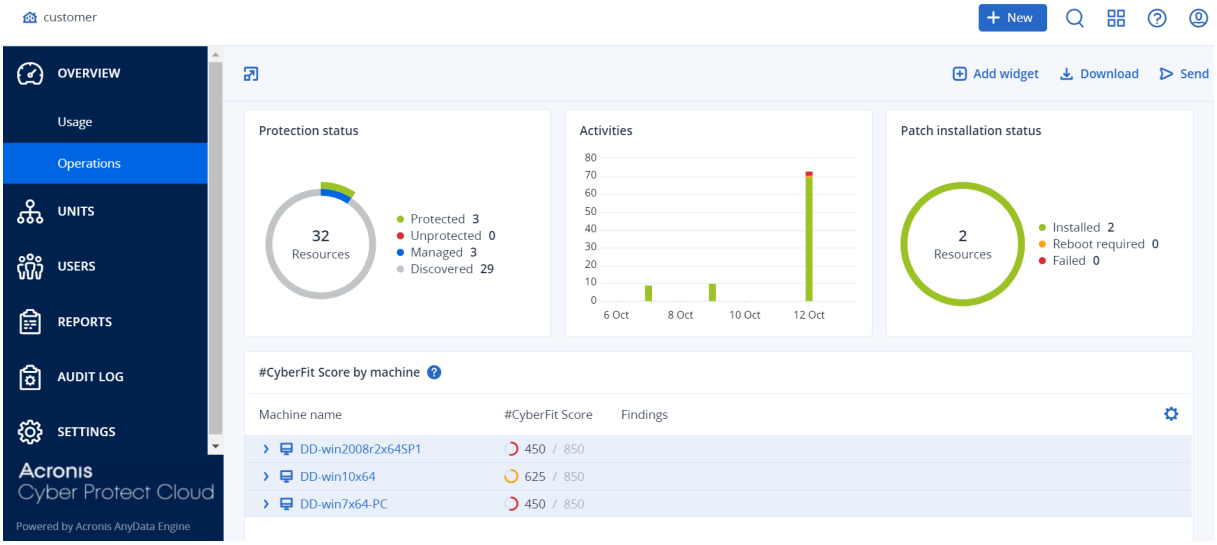
Tableau de bord des opérations

Le tableau de bord **Opérations** n'est disponible que pour les administrateurs d'entreprise lorsqu'ils travaillent à l'échelle de l'entreprise.

Le tableau de bord **Opérations** fournit un certain nombre de widgets personnalisables qui apporteront une vue d'ensemble des opérations liées au service Cyber Protection.

Les widgets sont mis à jour toutes les deux minutes. Les widgets disposent d'éléments sur lesquels cliquer qui permettent de faire des recherches sur les problèmes et de les résoudre. Vous pouvez télécharger l'état actuel du tableau de bord ou bien l'envoyer par courrier électronique au format .pdf et/ou .xlsx.

Vous pouvez faire un choix parmi de nombreux widgets se présentant sous la forme de tableaux, de diagrammes circulaires, de graphiques à barres, de listes et de cartes proportionnelles. Vous pouvez ajouter plusieurs widgets du même type en choisissant différents filtres.



Pour réorganiser les widgets sur le tableau de bord

Glissez-déplacez les widgets en cliquant sur leur nom.

Pour modifier un widget

Cliquez sur l'icône en forme de crayon à côté du nom du widget. Modifier un widget vous permet de le renommer, de modifier l'intervalle de temps et de définir des filtres.

Pour ajouter un widget

Cliquez sur **Ajouter widget**, puis effectuez l'une des actions suivantes :

- Cliquez sur le widget que vous désirez ajouter. Le widget sera ajouté avec les paramètres par défaut.
- Pour modifier le widget avant de l'ajouter, cliquez sur l'icône en forme de crayon lorsque le widget est sélectionné. Lorsque vous avez terminé de modifier le widget, cliquez sur **Terminé**.

Pour supprimer un widget

Cliquez sur le signe X à côté du nom du widget.

État de protection

État de protection

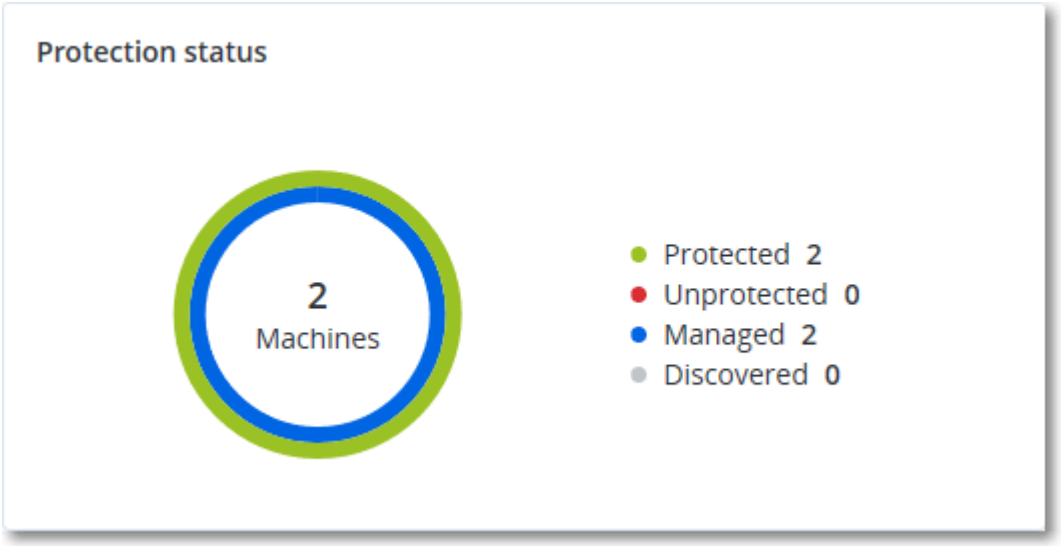
Ce widget affiche l'état de protection actuel de toutes les machines.

Une machine peut présenter l'un des états suivants :

- **Protégé** : machines sur lesquelles le plan de protection est appliqué.
- **Non protégé** : machines sur lesquelles le plan de protection n'est pas appliqué. Elles comprennent à la fois les machines découvertes et les machines gérées auxquelles aucun plan de protection n'est appliqué.

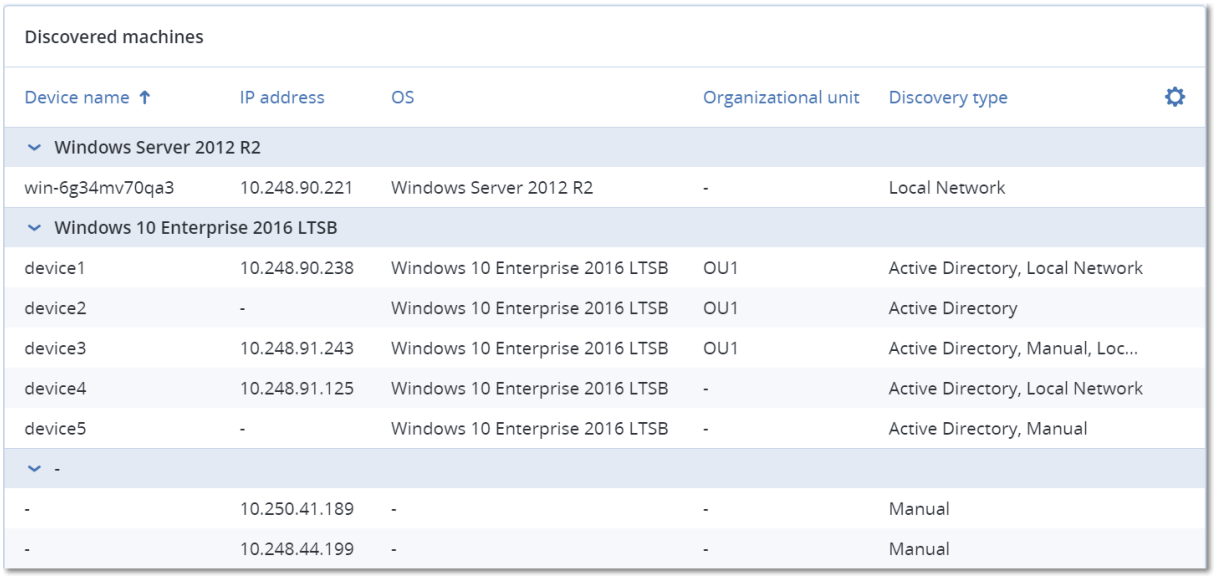
- **Géré** : machines sur lesquelles l'agent de protection est installé.
- **Découvert** : les machines sur lesquelles l'agent de protection n'est pas installé.

Si vous cliquez sur l'état de la machine, vous serez redirigé vers la liste des machines qui présentent le même état pour en savoir plus.



Machines découvertes

Ce widget affiche la liste des machines découvertes pendant la période spécifiée.


Discovered machines

Device name ↑	IP address	OS	Organizational unit	Discovery type
Windows Server 2012 R2				
win-6g34mv70qa3	10.248.90.221	Windows Server 2012 R2	-	Local Network
Windows 10 Enterprise 2016 LTSB				
device1	10.248.90.238	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Local Network
device2	-	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory
device3	10.248.91.243	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Manual, Loc...
device4	10.248.91.125	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Local Network
device5	-	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Manual
-				
-	10.250.41.189	-	-	Manual
-	10.248.44.199	-	-	Manual

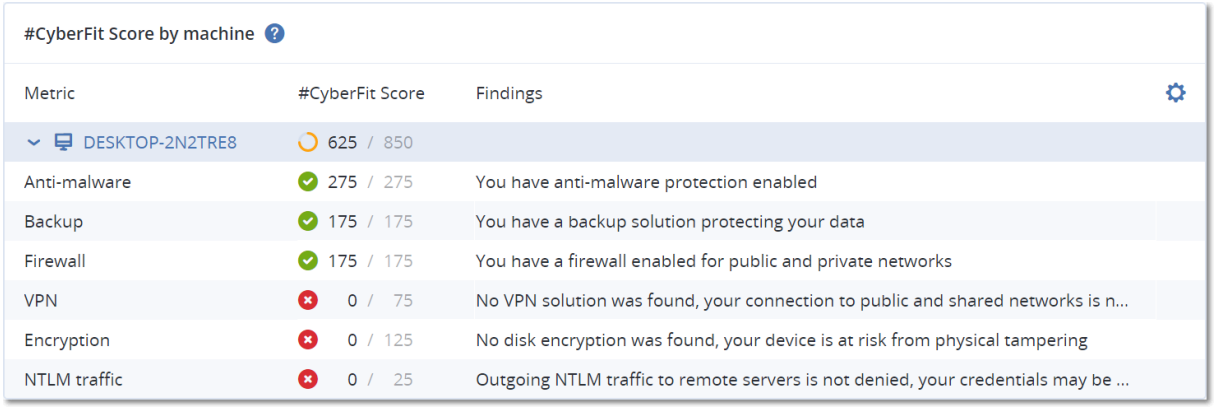
Score #CyberFit par machine

Ce widget affiche, pour chaque machine, le Score #CyberFit total, une combinaison de ses scores ainsi que les résultats pour chaque indicateur évalué :

- Anti-malware
- Sauvegarde
- Pare-feu
- VPN
- Chiffrement
- Trafic NTLM

Afin d'améliorer le score de chaque indicateur, vous pouvez afficher les recommandations disponibles dans le rapport.

Pour en savoir plus sur le Score #CyberFit, reportez-vous à « Score #CyberFit pour les machines ».



Widgets de protection évolutive des points de terminaison

Important
Il s'agit d'une version d'accès anticipé de la documentation sur la protection évolutive des points de terminaison. Certaines des fonctionnalités est descriptions sont peut-être incomplètes.

La protection évolutive des points de terminaison comprend un certain nombre de widgets qui sont accessibles depuis le tableau de bord **Opérations**.

Les widgets disponibles sont :

- Distribution des principaux incidents par ressource
- MTTR de l'incident
- Résolution des incidents de sécurité
- Statut réseau des ressources

Distribution des principaux incidents par ressource

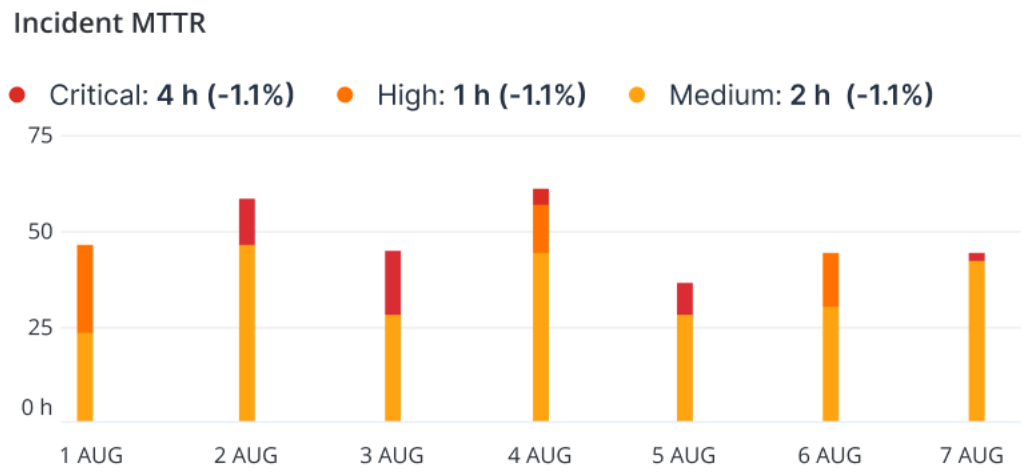
Ce widget affiche les cinq premières ressources qui comportent le plus d'incidents (cliquez sur **Afficher tout** pour rediriger l'utilisateur vers la liste des incidents ; elle est filtrée en fonction des paramètres du widget).

Survolez une ligne de ressource pour afficher le détail de l'état des enquêtes en cours menées sur les incidents ; les états d'enquête sont les suivants : **Non démarrée**, **Enquête en cours**, **Clôturée** et **Faux positif**. Cliquez ensuite sur la ressource que vous souhaitez analyser plus en détail, puis sélectionnez le client pertinent dans la fenêtre contextuelle qui s'affiche ; la liste des incidents est mise à jour en fonction des paramètres du widget.

MTTR de l'incident

Ce widget affiche le temps de résolution moyen des incidents de sécurité. Il indique la vitesse à laquelle les incidents font l'objet d'enquêtes et sont résolus.

Cliquez sur une colonne pour afficher le détail des incidents en fonction de la gravité (**Critique**, **Élevé** et **Moyen**), ainsi qu'une indication de la durée qui a été nécessaire à la résolution des différents niveaux de gravité. La valeur % figurant entre parenthèses indique l'augmentation ou la diminution par rapport à la période précédente.

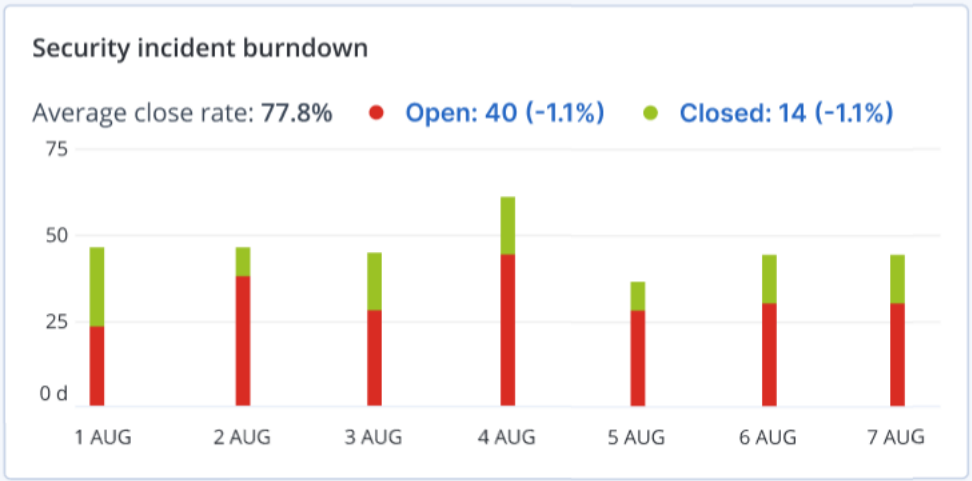


Résolution des incidents de sécurité

Ce widget indique l'efficacité de la clôture des incidents ; le nombre d'incidents ouverts est mesuré en fonction du nombre d'incidents clôturés pendant une période définie.

Survolez une colonne pour afficher le détail des incidents clôturés et ouverts pour le jour sélectionné. Si vous cliquez sur Ouvrir, une fenêtre contextuelle s'affiche dans laquelle vous pouvez y sélectionner le tenant approprié. La liste filtrée des incidents concernant le tenant sélectionné s'affiche et répertorie les incidents ouverts (état **Enquête en cours** ou **Non démarré**) Si vous cliquez sur Clôturé, la liste des incidents concernant le tenant sélectionné s'affiche et exclut les incidents qui ne sont plus ouverts (état **Clôturé** ou **Faux positif**).

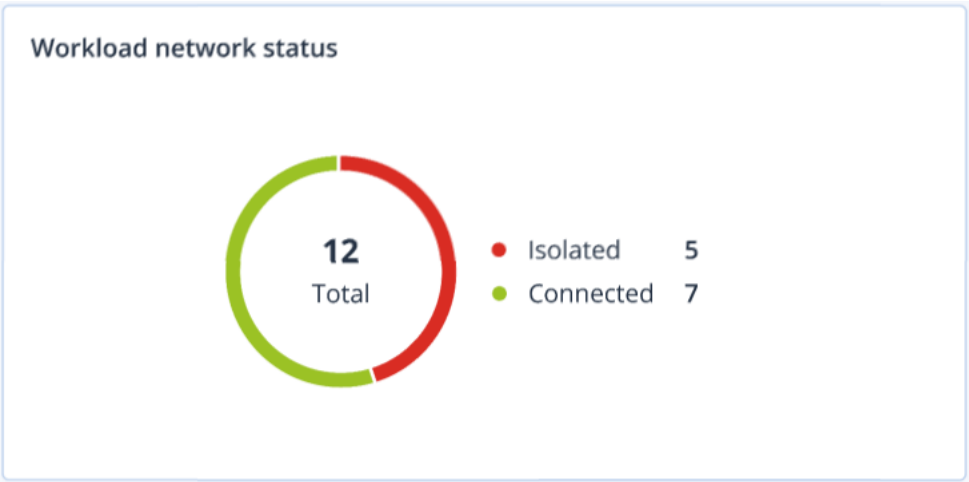
La valeur % figurant entre parenthèses indique l'augmentation ou la diminution par rapport à la période précédente.



Statut réseau des ressources

Ce widget affiche le statut réseau actuel de vos ressources ; il indique le nombre de ressources isolées et le nombre de ressources connectées.

Si vous cliquez sur Isolé, une fenêtre contextuelle s'affiche dans laquelle vous pouvez sélectionner le tenant approprié. La vue des ressources est filtrée et n'affiche que les ressources isolées. Cliquez sur la valeur Connecté pour afficher la liste des ressources avec agent qui ne répertorie que les ressources connectées (du tenant sélectionné).



Surveillance de l'intégrité du disque

La surveillance de l'intégrité du disque fournit des informations sur l'intégrité actuelle du disque, ainsi que des prévisions concernant cette dernière. Vous pouvez ainsi prévenir les pertes de données liées à une panne du disque. Les disques durs, tout comme les SSD, sont pris en charge.

Limites

- La prévision de l'intégrité du disque est prise en charge uniquement pour les ordinateurs Windows.
- Seuls les disques des machines physiques sont surveillés. Les disques des machines virtuelles ne peuvent pas être surveillés et ne s'affichent pas dans les widgets d'intégrité du disque.
- Les configurations RAID ne sont pas prises en charge. Les widgets d'intégrité du disque n'incluent aucune information sur les ordinateurs avec implémentation RAID.
- Les disques SSD NVMe ne sont pas supportés.

L'intégrité du disque est représentée par l'un des états suivants :

- **OK :**
  l'intégrité du disque est comprise entre 70 et 100 %.
- **Avertissement :**
  l'intégrité du disque est comprise entre 30 et 70 %.
- **Critique :**
  l'intégrité du disque est comprise entre 0 et 30 %.
- **Calcul des données du disque :**
  l'intégrité actuelle et la prévision de l'intégrité du disque sont en cours de calcul.

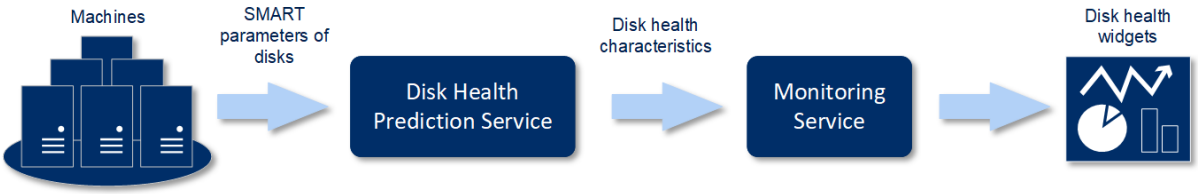
Fonctionnement

Le service Prévision de l'intégrité du disque se sert d'un modèle de prévision basé sur l'intelligence artificielle.

1. L'agent de protection collecte les paramètres SMART des disques et transmet ces données au service Prévision de l'intégrité du disque :
   - SMART 5 : nombre de secteurs réalloués.
   - SMART 9 : nombre d'heures de fonctionnement.
   - SMART 187 : nombre d'erreurs signalées qui n'ont pas été corrigées.
   - SMART 188 : expiration de commandes.
   - SMART 197 : nombre actuel de secteurs en attente.
   - SMART 198 : nombre de secteurs hors ligne impossible à corriger.
   - SMART 200 : taux d'erreurs d'écriture.

2. Le service Prévision de l'intégrité du disque traite les paramètres SMART reçus, effectue des prévisions, puis fournit les caractéristiques d'intégrité du disque suivantes :
   - État de santé actuel du disque : OK, Avertissement, Critique.
   - Prévision de l'état de santé du disque : négatif, stable, positif.
   - Probabilité de prévision de l'état de santé du disque en pourcentage.

   La période de prévision est d'un mois.
3. Le service de surveillance reçoit ces caractéristiques, puis affiche les informations pertinentes dans les widgets d'intégrité du disque dans la console Cyber Protect.



Widgets de l'état de santé du disque

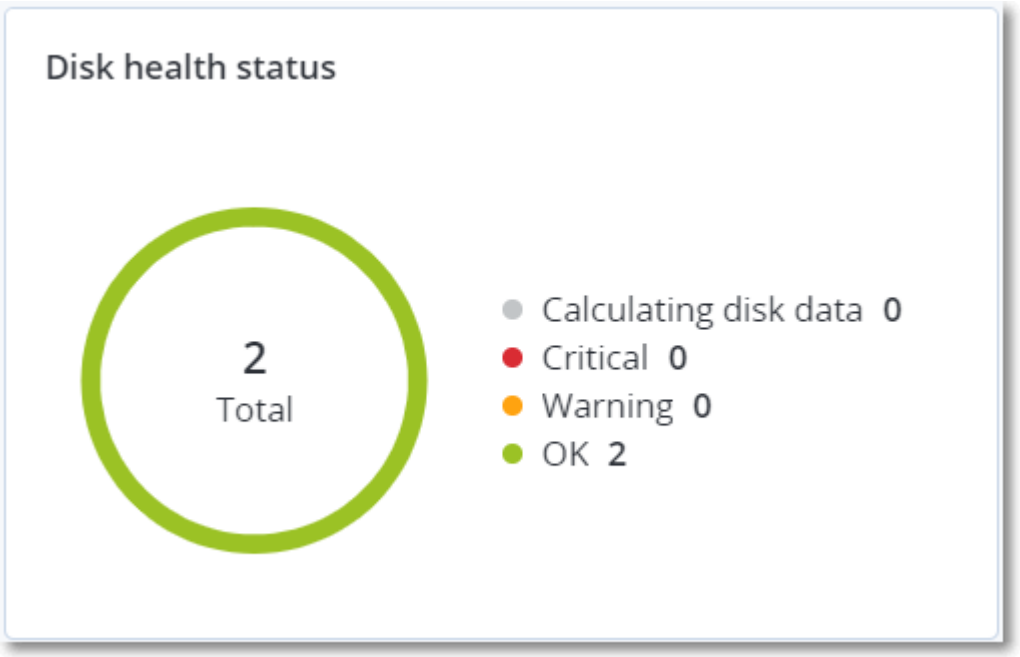
Les résultats de la surveillance de l'intégrité du disque sont présentés dans les widgets suivants, disponibles dans la console Cyber Protect.

- **Vue d'ensemble de l'intégrité du disque** est un widget en forme de carte proportionnelle, qui possède deux niveaux de détails que vous pouvez explorer :
  - Niveau ordinateur
    Affiche des informations résumées concernant l'intégrité du disque en fonction des ordinateurs client que vous avez sélectionnés. Seul l'état de disque le plus critique est affiché. Les autres états s'affichent dans une info-bulle lorsque vous passez le pointeur sur un bloc en particulier. La taille du bloc d'un ordinateur dépend de la taille totale de l'ensemble de ses disques. La couleur du bloc d'une machine dépend de l'état de disque le plus critique identifié.

- Niveau disque
  Affiche l'intégrité actuelle de tous les disques pour l'ordinateur sélectionné. Chaque bloc de disque affiche les prévisions d'intégrité du disque suivantes, ainsi que leur probabilité en pourcentage :
  - Sera altéré
  - Restera stable

- Sera amélioré

- **Intégrité du disque** est un widget de graphique circulaire qui affiche le nombre de disques pour chaque état.



Alertes relatives à l'état de santé du disque

La vérification de l'intégrité du disque est exécutée toutes les 30 minutes, alors que l'alerte correspondante n'est générée qu'une fois par jour. Lorsque l'intégrité du disque passe de **Avertissement** à **Critique**, une alerte est toujours générée.

Nom de l'alerte	La gravité	Intégrité du disque	Description
Une défaillance du disque dur est possible	Avertissement	(30 – 70)	Il est possible que le disque <nom du disque> sur cet ordinateur échoue à l'avenir. Exécutez une sauvegarde d'image complète du disque dès que possible, remplacez ce dernier, puis restaurez l'image sur le nouveau disque.
La défaillance du disque dur est imminente	Critique	(0 – 30)	Le disque <nom du disque> sur cet ordinateur est dans un état critique et risque fortement d'échouer très bientôt. Nous ne vous recommandons pas d'effectuer une sauvegarde d'image de ce disque à ce stade, car la contrainte supplémentaire risque de causer la défaillance du disque. Sauvegardez les fichiers les plus importants sur le disque dès maintenant et remplacez-le.

Carte de la protection des données

La fonctionnalité Carte de la protection des données vous permet de découvrir toutes les données qui ont une importance à vos yeux, et d'obtenir des informations détaillées concernant le nombre, la taille, l'emplacement et l'état de protection de tous les fichiers importants, le tout sous forme de carte proportionnelle dont vous pouvez faire varier l'échelle.

La taille de chaque bloc dépend du nombre total ou de la taille totale des fichiers importants qui appartiennent à un client ou à une machine.

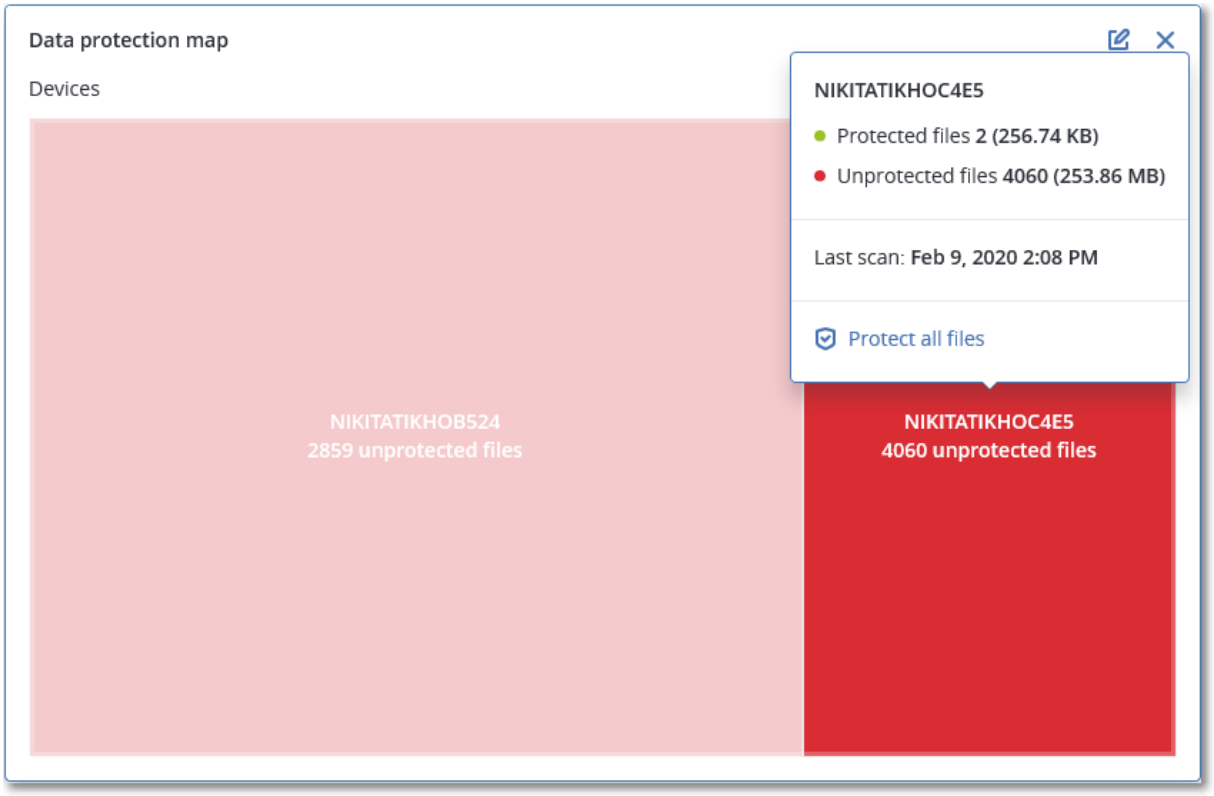
Les fichiers peuvent présenter l'un des états de protection suivants :

- **Critique** : de 51 à 100 % des fichiers non protégés et présentant l'extension que vous avez spécifiée ne sont pas sauvegardés et ne le seront pas non plus avec les paramètres de sauvegarde existants pour la machine ou l'emplacement sélectionné.
- **Basse** : de 21 à 50 % des fichiers non protégés et présentant l'extension que vous avez spécifiée ne sont pas sauvegardés et ne le seront pas non plus avec les paramètres de sauvegarde existants pour la machine ou l'emplacement sélectionné.
- **Moyen** : de 1 à 20 % des fichiers non protégés et présentant l'extension que vous avez spécifiée ne sont pas sauvegardés et ne le seront pas non plus avec les paramètres de sauvegarde existants pour la machine ou l'emplacement sélectionné.

- **Élevé** : tous les fichiers présentant l'extension que vous avez spécifiée sont protégés (sauvegardés) pour la machine ou l'emplacement sélectionné.

Les résultats de l'examen de la protection des données sont disponibles sur le tableau de bord dans le widget Carte de la protection des données, un widget sous forme de carte proportionnelle, qui permet d'afficher des informations au niveau machine :

- Niveau machine : affiche des informations concernant l'état de protection de fichiers importants en fonction des machines du client sélectionné.



Pour protéger des fichiers qui ne sont pas protégés, passez le pointeur de la souris sur le bloc, puis cliquez sur **Protéger tous les fichiers**. Dans la boîte de dialogue, vous trouverez des informations concernant le nombre de fichiers non protégés, ainsi que leur emplacement. Pour les protéger, cliquez sur **Protéger tous les fichiers**.

Vous pouvez aussi télécharger un rapport détaillé au format CSV.

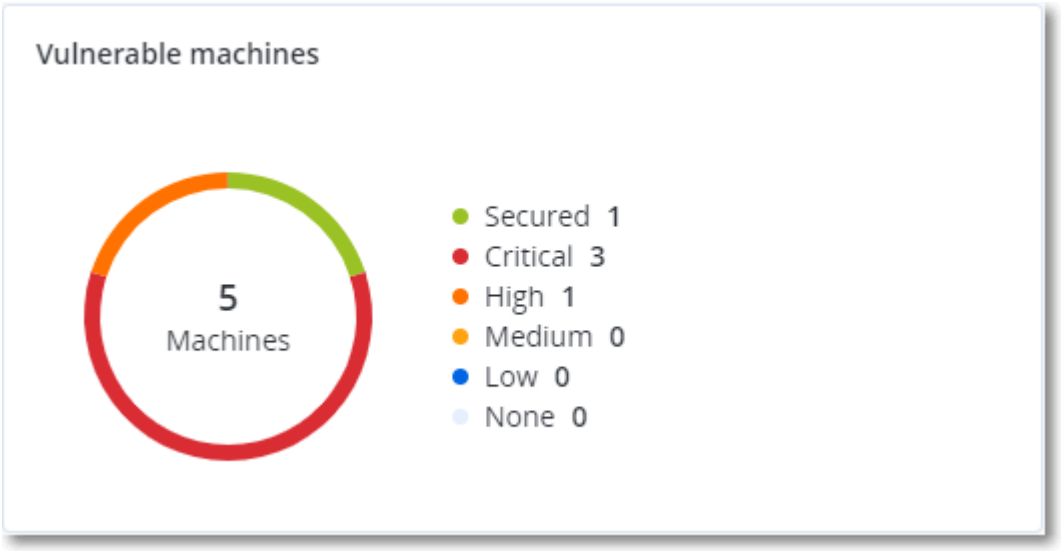
Widgets d'évaluation des vulnérabilités

Machines vulnérables

Ce widget affiche les ordinateurs vulnérables en les classant en fonction de la gravité de leur vulnérabilité.

La vulnérabilité découverte peut présenter l'un des niveaux de gravité suivants, d'après le système d'évaluation des vulnérabilités (CVSS) v3.0 :

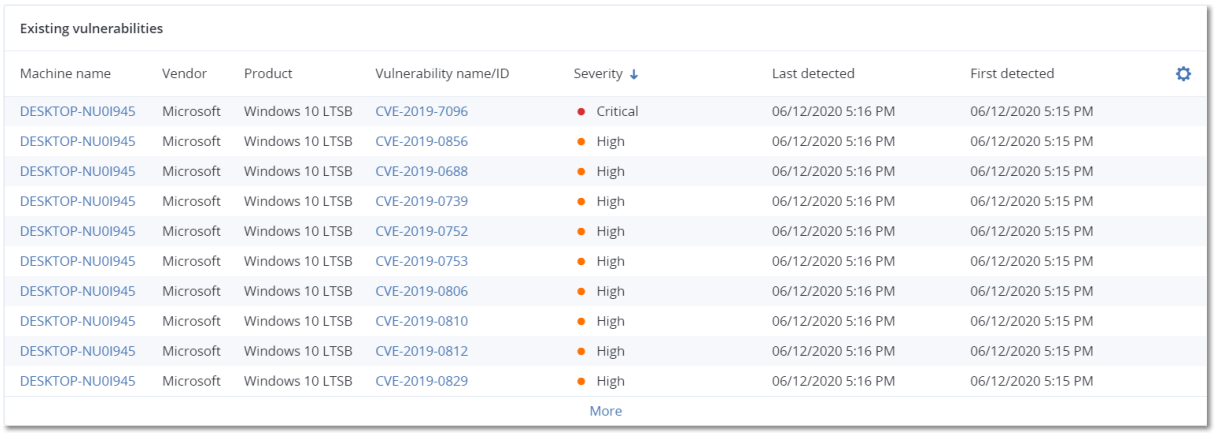
- Sécurisé : aucune vulnérabilité n'a été trouvée
- Critique : 9,0 – 10,0 CVSS
- Élevé : 7,0 – 8,9 CVSS
- Moyen : 4,0 – 6,9 CVSS
- Faible : 0,1 – 3,9 CVSS
- Aucun : 0,0 CVSS



Vulnérabilités existantes

Ce widget affiche les vulnérabilités existant actuellement sur les machines. Dans le widget **Vulnérabilités existantes**, il existe deux colonnes affichant la date et l'heure de la dernière modification :

- **Première détection** : date et heure à laquelle une vulnérabilité a initialement été détectée sur une machine.
- **Dernière détection** : date et heure à laquelle une vulnérabilité a été détectée sur une machine pour la dernière fois.


Existing vulnerabilities

Machine name	Vendor	Product	Vulnerability name/ID	Severity	Last detected	First detected
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-7096	Critical	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0856	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0688	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0739	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0752	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0753	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0806	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0810	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0812	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0829	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM

More

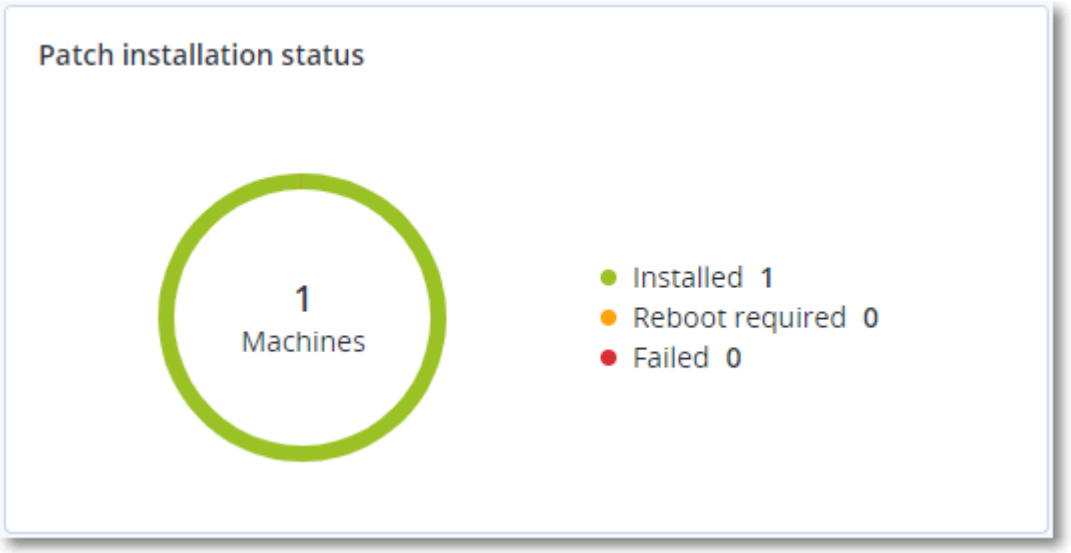
Widgets d'installation des correctifs

Il existe quatre widgets en lien avec la fonctionnalité de gestion des correctifs.

Statut d'installation des correctifs

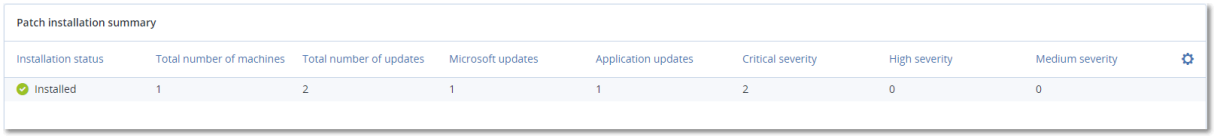
Ce widget affiche le nombre de machines, en les regroupant par statut d'installation des correctifs.

- **Installé :** tous les correctifs disponibles sont installés sur une machine.
- **Redémarrage nécessaire :** après l'installation des correctifs, un redémarrage est requis pour une machine.
- **Échec :** l'installation des correctifs sur une machine a échoué.



Résumé d'installation des correctifs

Ce widget affiche le résumé des correctifs sur les machines, en les regroupant par statut d'installation des correctifs.



Historique d'installation des correctifs

Ce widget affiche des informations détaillées au sujet des correctifs sur les machines.

Patch installation history

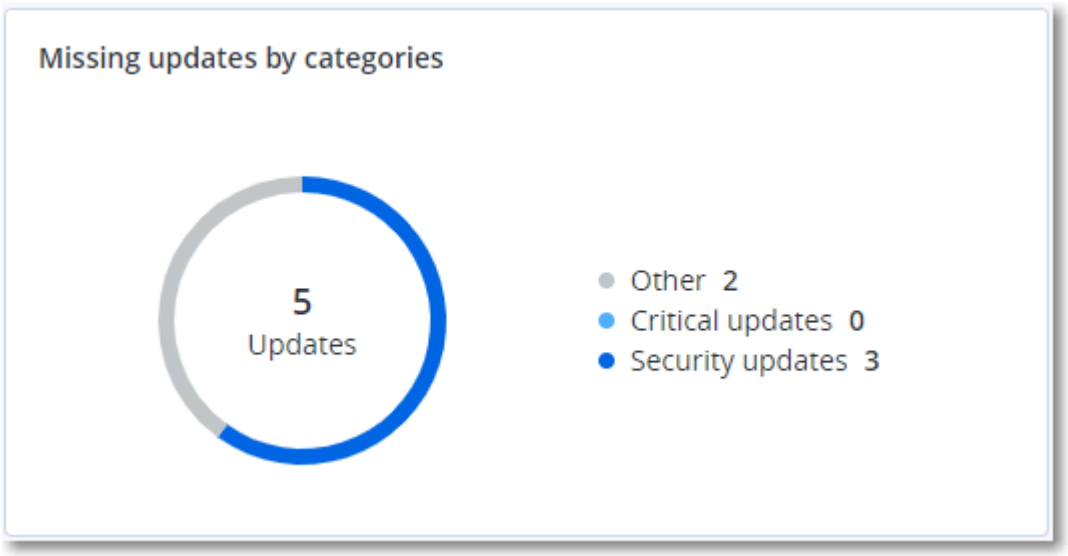
Machine name	Update name	Version	Severity	Approval status	Installation status	Installation date
NIKITATIKHOC4E5	FastStone Soft FastStone I...	5.9	Medium	New	Installed	02/05/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Oracle Java Runtime Envir...	8.0.2410.7	High	New	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020

More

Mises à jour manquantes, par catégorie

Ce widget affiche le nombre de mises à jour manquantes, en les classant par catégorie Les catégories suivantes sont répertoriées :

- Mises à jour de sécurité
- Mises à jour critiques
- Autre



Détails de l'analyse de la sauvegarde

Ce widget affiche des informations détaillées au sujet des menaces détectées dans les sauvegardes.

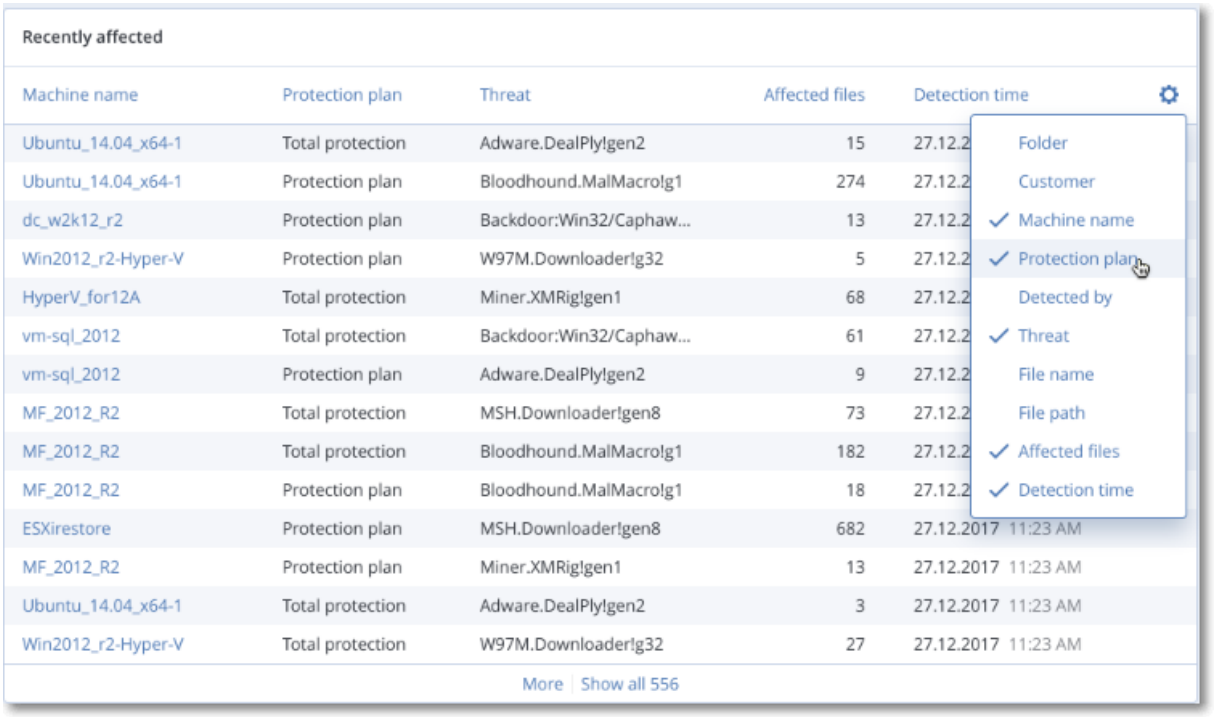
Backup scanning details (threats)

Device name	Plan name	Backup Date and time	Contents type	Location	Threat name	Affected files	Date and time
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:33 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:33 PM

More

Affectés récemment

Ce widget montre des informations détaillées au sujet des ressources touchées par des menaces telles que des virus, des malwares et des ransomwares. Vous y trouverez des informations concernant les menaces détectées, l'heure de détection et le nombre de fichiers touchés.



Téléchargement de données pour les ressources récemment affectées

Vous pouvez télécharger les données pour les ressources récemment affectées, générer un fichier CSV et l'envoyer aux destinataires que vous spécifiez.

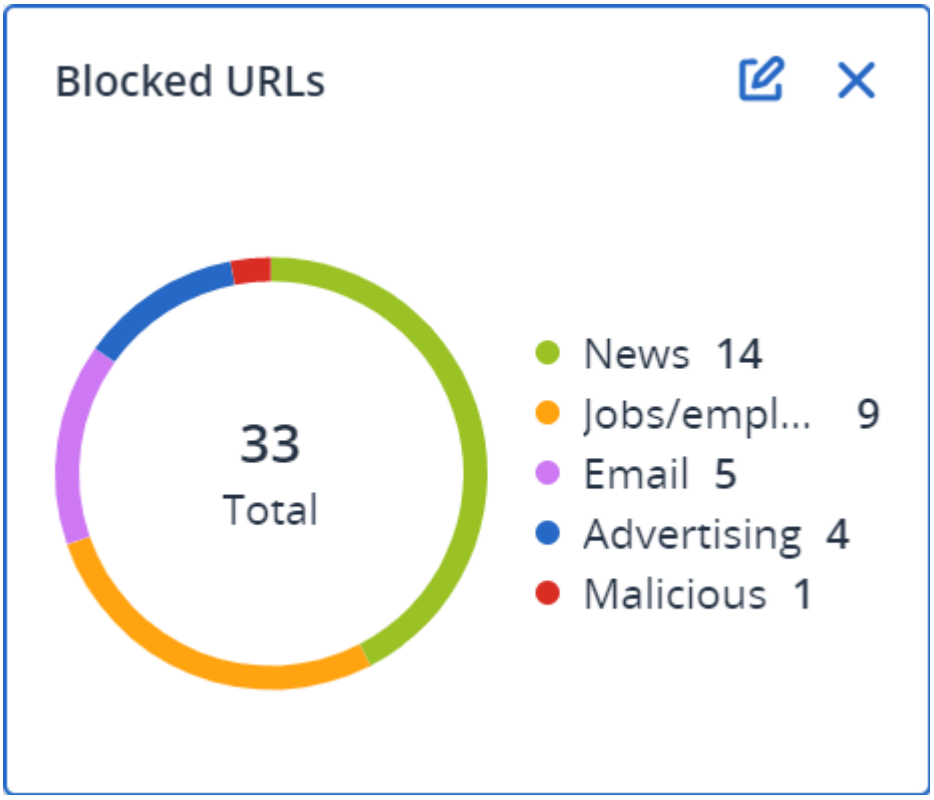
Pour télécharger les données pour les ressources récemment affectées

1. Dans le widget **Affectés récemment**, cliquez sur **Télécharger les données**.
2. Dans le champ **Période**, saisissez le nombre de jours pendant lequel vous souhaitez télécharger des données. Le nombre maximum de jours que vous pouvez entrer est 200.
3. Dans le champ **Destinataires**, saisissez l'adresse e-mail de toutes les personnes qui recevront un e-mail avec un lien pour télécharger le fichier CSV.
4. Cliquez sur **Télécharger**.

   Le système commence à générer le fichier CSV avec les données pour les ressources qui ont été affectées au cours de la période que vous avez spécifiée. Quand le fichier CSV est prêt, le système envoie un e-mail aux destinataires. Chaque destinataire peut ensuite télécharger le fichier CSV.

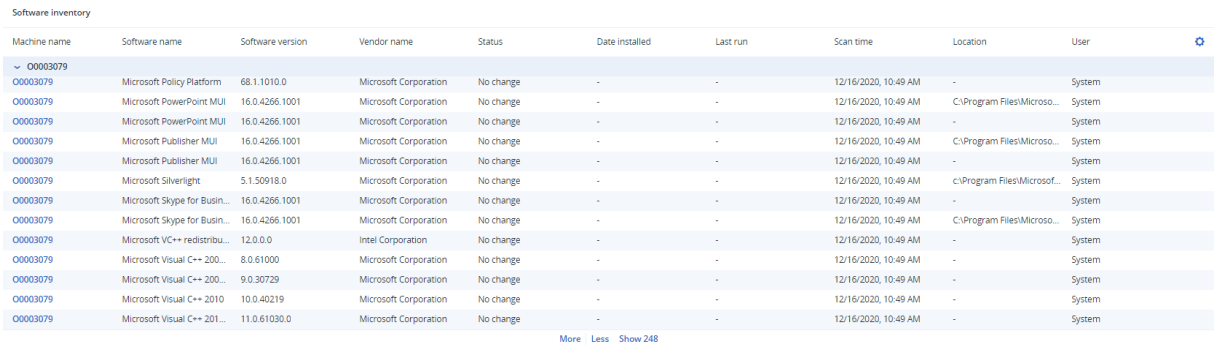
URL bloquées

Le widget affiche les statistiques des URL bloquées par catégorie. Pour en savoir plus sur le filtrage et la catégorisation des URL, consultez le Guide de l'utilisateur de Cyber Protect.



Widget d'inventaire du logiciel

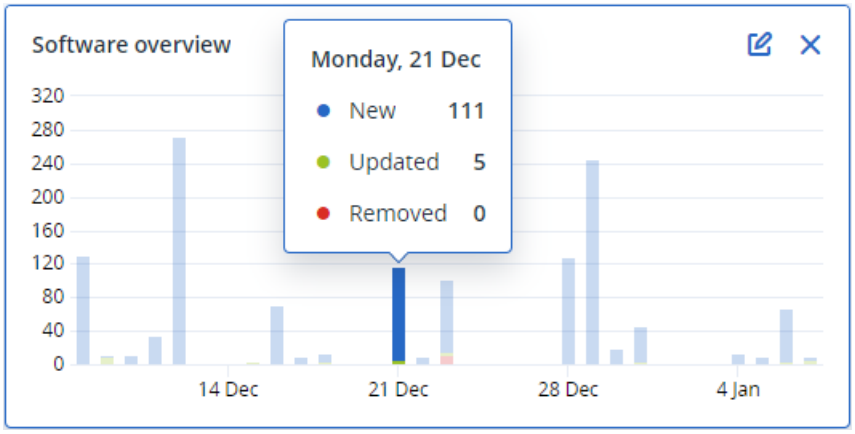
Le widget de tableau **Inventaire du logiciel** contient des informations détaillées concernant tout le logiciel installé sur les terminaux physiques Windows et macOS de votre organisation.


Software inventory

Machine name	Software name	Software version	Vendor name	Status	Date installed	Last run	Scan time	Location	User
O0003079									
O0003079	Microsoft Policy Platform	68.1.1010.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft PowerPoint MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
O0003079	Microsoft PowerPoint MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Publisher MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
O0003079	Microsoft Publisher MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Silverlight	5.1.50918.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	c:\Program Files\Microsof...	System
O0003079	Microsoft Skype for Busin...	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Skype for Busin...	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
O0003079	Microsoft VC++ redistribu...	12.0.0.0	Intel Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Visual C++ 200...	8.0.61000	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Visual C++ 200...	9.0.30729	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Visual C++ 2010	10.0.40219	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Visual C++ 201...	11.0.61030.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System

More Less Show 248

Le widget **Aperçu du logiciel** contient le nombre de nouvelles applications ou d'applications mises à jour et supprimées sur les terminaux physiques Windows et macOS de votre organisation sur une période donnée (7 jours, 30 jours ou le mois en cours).



Lorsque vous passez le pointeur sur une barre en particulier, une infobulle contenant les informations suivantes s'affiche :

Nouvelles – le nombre d'applications nouvellement installées.

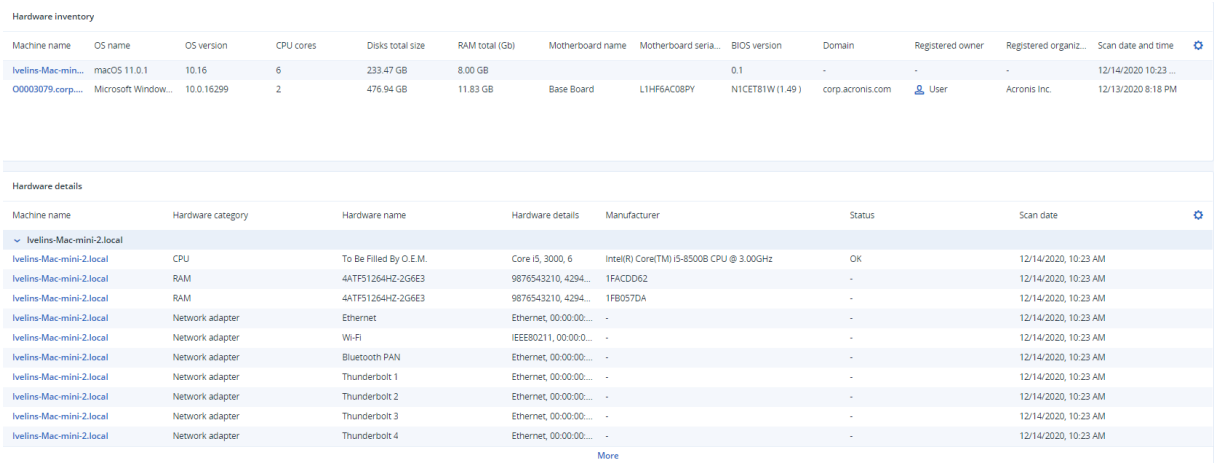
Mises à jour – le nombre d'applications mises à jour.

Supprimées – le nombre d'applications supprimées.

Lorsque vous cliquez sur la partie de la barre correspondant à un certain statut, vous êtes redirigé vers la page **Gestion de logiciel** -> **Inventaire du logiciel**. Les informations de cette page sont filtrées en fonction de la date et du statut correspondants.

Widgets d'inventaire du matériel

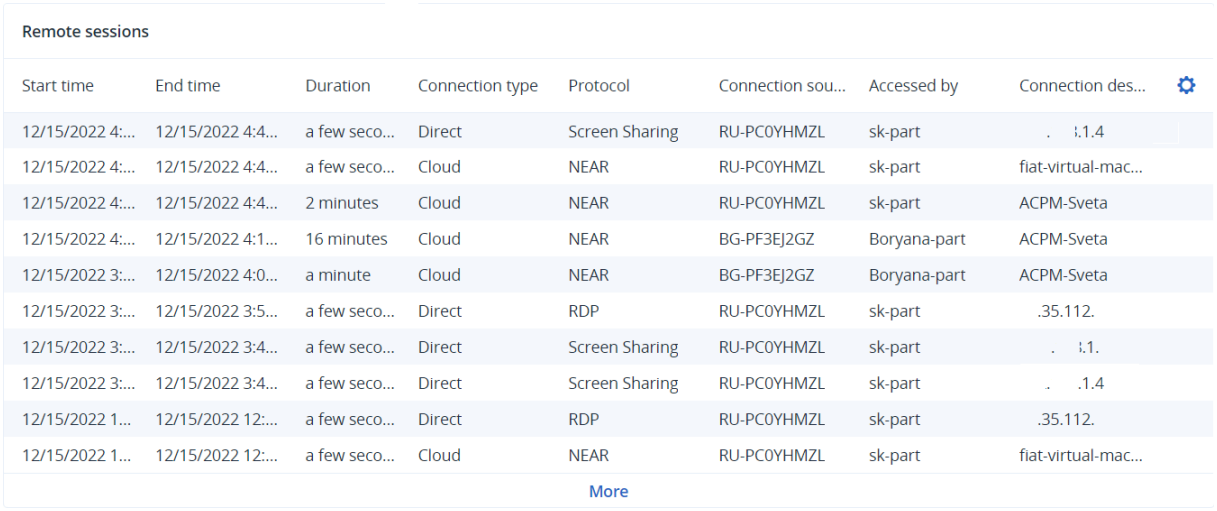
Les widgets de tableau **Inventaire du matériel** et **Détails du matériel** contiennent des informations concernant tout le matériel installé sur les terminaux physiques et virtuels Windows et macOS de votre organisation.



Le widget de tableau **Modifications apportées au matériel** contient des informations concernant le matériel ajouté, supprimé et modifié sur les terminaux physiques et virtuels Windows et macOS de votre organisation sur une période donnée (7 jours, 30 jours ou le mois en cours).

Historique des sessions

Le widget affiche les informations détaillées concernant les sessions Bureau à distance et transfert de fichiers effectuées dans votre organisation pendant une période spécifiée.



Journal d'audit

Pour afficher le journal d'audit, cliquez sur **Surveillance** > **Journal d'audit**.

Le journal d'audit fournit un enregistrement chronologique des événements suivants :

- Opérations effectuées par les utilisateurs dans le portail de gestion
- Opérations avec des ressources de cloud à cloud effectuées par des utilisateurs dans la console Cyber Protect
- Opérations de création de cyberscripts effectuées par des utilisateurs dans la console Cyber Protect
- Messages système concernant les quotas atteints et l'utilisation des quotas

Le journal affiche les événements de l'organisation ou de l'unité dans laquelle vous fonctionnez actuellement, et de ses unités enfant. Vous pouvez cliquer sur un événement pour afficher davantage d'informations le concernant.

Les journaux d'audit sont stockés dans le centre de données, et leur disponibilité ne peut pas être affectée par des problèmes survenant sur les ordinateurs de l'utilisateur final.

Le journal est nettoyé quotidiennement. Les événements sont supprimés au bout de 180 jours.

Champs de journal d'audit

Pour chaque événement, le journal affiche :

- **Evénement**
  Courte description de l'événement. Par exemple, **Tenant créé**, **Tenant supprimé**, **Utilisateur créé**, **Utilisateur supprimé**, **Le quota est atteint**, **Le contenu de la sauvegarde a été parcouru**, **Le script a été modifié**.
- **Gravité**
  Peut être l'une des options suivantes :
  - **Erreur**
    Indique une erreur.
  - **Avertissement**
    Indique une action négative potentielle. Par exemple, **Tenant supprimé**, **Utilisateur supprimé**, **Le quota est atteint**.
  - **Mentions légales**
    Indique un événement qui peut nécessiter votre attention. Par exemple, **Tenant a été mis à jour**, **Utilisateur mis à jour**.
  - **Informations**
    Indique un changement ou une action informatifs neutres. Par exemple, **Tenant créé**, **Utilisateur créé**, **Le quota a été mis à jour**, **Le plan de création de script a été supprimé**.
- **Date**
  Date et heure auxquelles l'événement a eu lieu.
- **Nom d'objet**
  Objet avec lequel l'opération a été effectuée. Par exemple, l'objet de l'événement **Utilisateur mis à jour** est l'utilisateur dont les propriétés ont été modifiées. Pour les événements associés à un quota, le quota est l'objet.
- **Tenant**
  Nom de l’unité à laquelle l'objet appartient. Par exemple, le tenant de l'événement **Utilisateur mis à jour** est l'unité dans laquelle l'utilisateur est situé. Le tenant de l'événement **Le quota est atteint** est l'utilisateur dont le quota a été atteint.
- **Initiateur**
  Identifiant de l’utilisateur qui a initié l'événement. Pour les messages système et événements initiés par des administrateurs de haut niveau, l'initiateur est affiché comme **Système**.
- **Initiateur du tenant**
  Nom de l'unité à laquelle l'initiateur appartient. Pour les messages système et les événements initiés par des administrateurs de haut niveau, le champ est vide.

- **Méthode**
  Indique si l'événement a été initié via l'interface Web ou via l'API.
- **IP**
  L'adresse IP de la machine à partir de laquelle l'événement a été initié.

Filtrer et rechercher

Vous pouvez filtrer les événements par type, gravité ou date. Vous pouvez également rechercher les événements par nom, objet, tenant, initiateur et initiateur du tenant.

Rapports

Pour accéder aux rapports relatifs à l'utilisation du service et aux opérations, cliquez sur **Rapports**.

Remarque
Cette fonctionnalité n'est pas disponible dans les éditions Standard du service Cyber Protection.

Rapports d'utilisation

Les rapports d'utilisation fournissent des données historiques sur l'utilisation des services. Les rapports d'utilisation sont disponibles aussi bien au format CSV qu'au format HTML.

Type de rapport

Vous pouvez sélectionner l'un des types de rapports suivants :

- **Utilisation actuelle**
  Ce rapport contient les mesures de l'utilisation actuelle du service.
- **Résumé pour cette période**
  Ce rapport contient les indicateurs de l'utilisation du service pour la fin de la période spécifiée, et la différence entre les mesures au début et à la fin de la période spécifiée.
- **Jour par jour pour cette période**
  Ce rapport contient les indicateurs de l'utilisation du service et leurs changements pour chaque jour de la période spécifiée.

Champ d'application du rapport

Vous pouvez choisir le champ d'application du rapport parmi les valeurs suivantes :

- **Clients directs et partenaires**
  Le rapport comprendra uniquement les mesures d'utilisation de service pour les unités enfants immédiates de la société ou de l'unité dans laquelle vous travaillez.
- **Tous les clients et partenaires**
  Le rapport comprendra les mesures d'utilisation de service pour les unités enfants de la société ou de l'unité dans laquelle vous travaillez.
- **Tous les clients et partenaires (y compris les informations d'utilisateur)**
  Le rapport comprendra les mesures d'utilisation de service pour les unités enfants de la société ou de l'unité dans laquelle vous travaillez, et pour tous les utilisateurs au sein des unités.

Indicateurs avec zéro utilisation

Vous pouvez réduire le nombre de lignes présentées dans le rapport en masquant les informations relatives aux indicateurs avec zéro utilisation.

Configuration de rapports d'utilisation planifiés

Un rapport planifié regroupe les mesures d'utilisation du service pour le mois précédent complet. Les rapports sont générés à 23:59:59 (UTC) le premier jour du mois et sont envoyés le second jour de ce même mois. Ils sont envoyés à tous les administrateurs de votre entreprise ou de votre unité qui ont sélectionné la case à cocher **Rapports d'utilisation planifiés** dans leurs paramètres utilisateur.

Pour activer ou désactiver un rapport planifié

1. Connectez-vous au portail de gestion.
2. Assurez-vous de travailler dans la société ou l'unité la plus haute disponible.
3. Cliquez sur **Rapports** > **Utilisation**.
4. Cliquez sur **Planifié**.
5. Cochez ou décochez la case **Envoyer un rapport de synthèse mensuel**.
6. Dans **Niveau de détail**, sélectionnez le champ d'application du rapport.
7. [Facultatif] Sélectionnez **Masquer les indicateurs avec zéro utilisation** si vous souhaitez exclure du rapport les indicateurs avec zéro utilisation.

Configuration de rapports d'utilisation personnalisés

Un rapport personnalisé est généré à la demande et ne peut être planifié. Le rapport sera envoyé à votre adresse e-mail.

Pour générer un rapport personnalisé

1. Connectez-vous au portail de gestion.
2. Naviguez vers l'unité pour laquelle vous souhaitez créer un rapport.
3. Cliquez sur **Rapports** > **Utilisation**.
4. Cliquez sur **Personnalisé**.
5. Dans **Type**, sélectionnez le type de rapport.
6. [Non disponible pour le type de rapport **d'utilisation actuelle**] Dans **Période**, sélectionnez la période couverte par le rapport :
   - **Mois actuel**
   - **Mois précédent**
   - **Personnalisé**
7. [Non disponible pour le type de rapport **d'utilisation actuelle**] Si vous souhaitez indiquer une période de rapport personnalisée, sélectionnez les dates de début et de fin. Sinon, ignorez cette étape.
8. Dans **Niveau de détail**, sélectionnez le champ d'application du rapport.

9. [Facultatif] Sélectionnez **Masquer les indicateurs avec zéro utilisation** si vous souhaitez exclure du rapport les indicateurs avec zéro utilisation.
10. Pour générer le rapport, cliquez sur **Générer et envoyer**.

Données des rapports d'utilisation

Le rapport sur l'utilisation du service Cyber Protection comprend les informations suivantes à propos d'une entreprise ou d'une unité :

- Le volume des sauvegardes par unité, par utilisateur et par type de terminal.
- Le nombre de terminaux protégés par unité, par utilisateur et par type de terminal.
- La valeur par unité, par utilisateur et par type de terminal.
- Le volume total de sauvegardes.
- Le nombre total de terminaux protégés.
- La valeur totale.

Remarque
Si le service Cyber Protection ne parvient pas à détecter un type de terminal, ce terminal apparaît comme **Sans type** dans le rapport.

Rapports d'opération

Les rapports **Opérations** ne sont disponibles que pour les administrateurs d'entreprise lorsqu'ils travaillent à l'échelle de l'entreprise.

Un rapport au sujet des opérations peut inclure n'importe quel ensemble de widgets du tableau de bord **Opérations**. Tous les widgets présentent le résumé pour l'ensemble de l'entreprise.
En fonction du type de widget, le rapport inclut les données pour une période ou pour le moment de la navigation ou de la génération de rapport. Consultez "Données rapportées en fonction du type de widget" (p. 84).

Tous les widgets historiques présentent les données pour le même intervalle de temps. Vous pouvez modifier cela dans les paramètres de rapport.

Vous pouvez utiliser des rapports par défaut ou créer un rapport personnalisé.

Vous pouvez télécharger un rapport ou l'envoyer par e-mail au format Excel (XLSX) ou PDF.

Les rapports par défaut sont répertoriés ci-dessous :

Nom du rapport	Description
Score #CyberFit par machine	Affiche le score #CyberFit basé sur l'évaluation des indicateurs et des configurations de sécurité pour chaque machine, ainsi que des recommandations d'amélioration.

Alertes	Affiche les alertes survenues pendant une période donnée.
Détails de l'analyse de la sauvegarde	Affiche des informations détaillées au sujet des menaces détectées dans les sauvegardes.
Activités quotidiennes	Affiche des informations résumées au sujet des activités réalisées lors d'une période donnée.
Carte de la protection des données	Affiche des informations détaillées concernant le nombre, la taille, l'emplacement et l'état de protection de tous les fichiers importants présents sur des machines.
Menaces détectées	Affiche les détails des machines affectées en les classant par nombre de menaces bloquées, ainsi que le nombre de machines saines et vulnérables.
Machines découvertes	Affiche toutes les machines trouvées dans le réseau de l'organisation.
Prévision de l'état de santé du disque	Affiche des prévisions concernant le moment où votre disque dur/SSD tombera en panne, ainsi que l'état actuel des disques.
Vulnérabilités existantes	Affiche les vulnérabilités existantes pour le système d'exploitation et les applications dans votre organisation. Le rapport affiche également les détails des machines affectées dans votre réseau pour chaque produit répertorié.
Résumé de la gestion des correctifs	Affiche le nombre de correctifs manquants, installés et applicables. Vous pouvez explorer les rapports pour obtenir des informations sur les correctifs manquants/installés, ainsi que sur tous les systèmes
Résumé	Affiche des informations résumées au sujet des terminaux protégés pendant une période donnée.
Activités hebdomadaires	Affiche des informations résumées au sujet des activités réalisées lors d'une période donnée.
Inventaire du logiciel	Affiche des informations détaillées concernant tout le logiciel installé sur les ordinateurs Windows et macOS de votre organisation.
Inventaire du matériel	Affiche des informations détaillées concernant tout le matériel disponible sur les ordinateurs physiques et virtuels Windows et macOS de votre organisation.
Sessions distantes	Affiche les informations détaillées concernant les sessions Bureau à distance et transfert de fichiers effectuées dans votre organisation pendant une période spécifiée.

Actions relatives aux rapports

Pour afficher un rapport, cliquez sur son nom.

Pour ajouter un nouveau rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Au bas de la liste des rapports disponibles, cliquez sur **Ajouter un rapport**.
3. [Pour ajouter un rapport prédéfini] Cliquez sur le nom du rapport prédéfini.
4. [Pour ajouter un rapport personnalisé] Cliquez sur **Personnalisé**, puis ajoutez des widgets au rapport.
5. [Facultatif] Glissez-déplacez les widgets pour les réorganiser.

Pour modifier un rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport que vous souhaitez modifier.
   Vous pouvez effectuer les opérations suivantes :
   - Renommer le rapport.
   - Modifier l'intervalle de temps de tous les widgets du rapport.
   - Spécifier les destinataires du rapport, ainsi que le moment où le rapport leur sera envoyé. Les formats disponibles sont PDF et XLSX.

Pour supprimer un rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport que vous souhaitez supprimer.
3. Cliquez sur l'icône représentant des points de suspension (...), puis cliquez sur **Supprimer**.
4. Confirmez votre choix en cliquant sur **Supprimer**.

Pour planifier un rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport que vous souhaitez planifier, puis cliquez sur **Paramètres**.
3. Activez le commutateur **Planifié**.
   - Spécifiez l'adresse e-mail des destinataires.
   - Sélectionnez le format du rapport.

   Remarque
   Vous pouvez exporter jusqu'à 1 000 éléments dans un fichier PDF et jusqu'à 10 000 éléments dans un fichier XLSX. Les horodatages des fichiers PDF et XLSX utilisent l'heure locale de votre ordinateur.

- Sélectionnez la langue du rapport.
- Configurez la planification.

4. Cliquez sur **Enregistrer**.

Pour télécharger un rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport, puis cliquez sur **Télécharger**.
3. Sélectionnez le format du rapport.

Pour envoyer un rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport, puis cliquez sur **Envoyer**.
3. Spécifiez l'adresse e-mail des destinataires.
4. Sélectionnez le format du rapport.
5. Cliquez sur **Envoyer**.

Pour exporter la structure des rapports

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport.
3. Cliquez sur l'icône représentant des points de suspension (...), puis cliquez sur **Exporter**.

En conséquence, la structure du rapport est enregistrée sur votre ordinateur en tant que fichier JSON.

Pour vider les données du rapport

En utilisant cette option, vous pouvez exporter toutes les données d'une période personnalisée, sans la filtrer, vers un fichier CSV et envoyer ce fichier par e-mail vers un destinataire.

Remarque
Vous pouvez exporter jusqu'à 150 000 éléments dans un fichier CSV. Les horodatages dans le fichier CSV utilisent le temps universel coordonné (UTC).

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport dont vous souhaitez vider les données.
3. Cliquez sur l'icône représentant des points de suspension (...), puis cliquez sur **Vider les données**.
4. Spécifiez l'adresse e-mail des destinataires.
5. Dans la zone **Plage de temps**, spécifiez la période personnalisée pour laquelle vous souhaitez vider les données.

Remarque
La préparation des fichiers CSV pour de plus longues périodes prend plus de temps.

6. Cliquez sur **Envoyer**.

Synthèse

Le rapport de synthèse fournit une vue d'ensemble du statut de protection de l'environnement de votre organisation et des terminaux protégés pour une période spécifiée.

Le rapport de synthèse inclut des sections personnalisables avec des widgets dynamiques, qui affichent les indicateurs de performances clés liés à votre utilisation des services Cloud suivants : Sauvegarde, Protection antimalware, Évaluation de la vulnérabilité, Gestion des correctifs, Notary, Reprise d'activité après sinistre et File Sync & Share.

Vous pouvez personnaliser le rapport de différentes manières.

- Ajouter ou supprimer des sections.
- Changer l'ordre des sections.
- Renommer des sections.
- Déplacer des widgets d'une section à une autre.
- En changeant l'ordre des widgets de chaque section.
- En ajoutant ou en supprimant des widgets.
- En personnalisant les widgets.

Vous pouvez générer des rapports de synthèse aux formats PDF et Excel et les envoyer aux parties prenantes ou propriétaires de votre organisation afin qu'ils puissent facilement consulter les indicateurs techniques et commerciaux relatifs aux services fournis.

Widgets de synthèse

Vous pouvez supprimer ou ajouter des sections et widgets du rapport de synthèse. Cela permet de définir les informations qui y sont incluses.

Widgets d'aperçu des ressources

Le tableau suivant fournit plus de détails sur les widgets de la section **Aperçu des ressources**.

Widget	Description
Statut de protection des ressources Cloud	Ce widget indique le nombre de ressources cloud protégées et non protégées par type au moment de la génération du rapport. Une ressource Cloud est considérée comme protégée si au moins un plan de protection ou de sauvegarde lui est appliqué. Une ressource Cloud est considérée comme non protégée si aucun plan de protection ou de

Widget	Description
	sauvegarde ne lui est appliqué. Les types de ressources Cloud suivants sont référencés dans le graphique (dans l'ordre alphabétique, de A à Z) : • Drive Google Workspace • Gmail Google Workspace • Drive partagé Google Workspace • Boîtes aux lettres Exchange hébergées • Boîtes aux lettres Microsoft 365 • Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams • Sites Web Pour certains types de ressources, les groupes de ressources suivants sont utilisés : • Microsoft 365 : Utilisateurs, Groupes, Dossiers publics, Équipes et Collections de sites • Google Workspace : Utilisateurs et Disques partagés • Exchange hébergé : Utilisateurs Si l'un des groupes de ressource contient plus de 10 000 ressources, le widget n'affiche pas de données correspondant à ces ressources. Par exemple, si le client possède un compte Microsoft 365 avec 10 000 boîtes aux lettres et le service OneDrive pour 500 utilisateurs, étant donné que le tout est comptabilisé dans le même groupe de ressource utilisateurs, la somme de ces ressources est 10 500, ce qui dépasse la limite de 10 000 pour un groupe de ressources. Le widget n'affichera donc pas les types de ressources correspondants : Boîtes aux lettres Microsoft 365 et OneDrive Microsoft 365.
Résumé Cyber Protection	Ce widget affiche les indicateurs de performance clés de la cyberprotection pour une période spécifiée. **Données sauvegardées** : taille totale des archives créées dans les stockages local et Cloud. **Menaces atténuées** : nombre total de malware bloqués sur l'ensemble des terminaux. **URL malveillantes bloquées** : nombre total d'URL bloquées sur l'ensemble des terminaux. **Vulnérabilités corrigées** : nombre total de vulnérabilités qui ont été corrigées par l'installation de correctifs logiciels sur l'ensemble des terminaux. **Correctifs installés** : nombre total de correctifs installés sur l'ensemble des terminaux.

Widget	Description
	Serveurs protégés par la RAS : nombre total de serveurs protégés par la reprise d'activité après sinistre. **Utilisateurs File Sync & Share** : nombre total des utilisateurs finaux et invités qui utilisent Cyber Files. **Fichiers notarisés** : nombre total de fichiers notarisés. **Documents signés de façon électronique** : nombre total de documents signés de façon électronique. **Périphériques bloqués** : nombre total de périphériques bloqués.
Statut réseau des ressources	Ce widget affiche le nombre de ressources isolées et le nombre de ressources connectées (état normal des ressources). Sélectionnez le client pertinent ; la vue des ressources est filtrée et n'affiche que les ressources isolées. Cliquez sur Connecté pour afficher la liste des ressources avec agent qui ne répertorie que les ressources connectées (du client sélectionné).
Statut de protection des ressources	Ce widget indique le nombre de ressources protégées et non protégées par type au moment de la génération du rapport. Une ressource est considérée comme protégée si au moins un plan de protection ou de sauvegarde lui est appliqué. Une ressource est considérée comme non protégée si aucun plan de protection ou de sauvegarde ne lui est appliqué. Les ressources suivantes sont prises en compte : **Serveurs** : serveurs physiques et serveurs contrôleur de domaine. **Stations de travail** : stations de travail physiques. **Machines virtuelles** : machines virtuelles avec agent et sans agent. **Serveurs d'hébergement Web** : serveurs virtuels or physiques avec cPanel ou Plesk installé. **Terminaux mobiles** : terminaux mobiles physiques. Une ressource peut appartenir à plusieurs catégories. Par exemple, un serveur d'hébergement Web est compté dans deux catégories : **Serveurs** et **Serveurs d'hébergement Web**.

Widgets de protection antimalware

Le tableau suivant fournit plus de détails sur les widgets de la section **Défense contre les menaces**.

Widget	Description
Analyse antimalware des fichiers	Ce widget affiche les résultats des analyses antimalware effectuées à la demande sur les terminaux pour une période spécifiée. **Fichiers** : nombre total de fichiers analysés

Widget	Description
	Propres : nombre total de fichiers propres **Détectés, mis en quarantaine** : nombre total de fichiers infectés mis en quarantaine **Détectés, non mis en quarantaine** : nombre total de fichiers infectés, non mis en quarantaine **Terminaux protégés** : nombre total de terminaux auxquels une règle de protection antimalware est appliquée **Total de terminaux enregistrés** : nombre total de terminaux enregistrés au moment de la génération du rapport
Analyse anti-malware des sauvegardes	Ce widget affiche les résultats des analyses antimalware des sauvegardes pour une période spécifiée, en utilisant les indicateurs suivants : • Nombre total de points de restauration analysés • Nombre de points de récupération propres • Nombre de points de récupération propres avec partitions non prises en charge • Nombre de points de récupération infectés. Cet indicateur inclut le nombre de points de récupération infectés avec partitions non prises en charge.
URL bloquées	Ce widget affiche les URL bloquées classées par catégorie de site Web pour une période spécifiée. Le widget liste les sept catégories de site Web qui totalisent le plus grand nombre d'URL bloquées. Les autres catégories sont regroupées dans la section **Autres**. Pour plus d'informations sur les catégories de site Web, consultez la section dédiée au filtrage des URL dans Cyber Protection.
Résolution des incidents de sécurité	Ce widget indique l'efficacité de la clôture des incidents pour la société sélectionnée ; le nombre d'incidents ouverts est mesuré en fonction du nombre d'incidents clôturés pendant une période définie. Survolez une colonne pour afficher le détail des incidents clôturés et ouverts pour le jour sélectionné. La valeur % figurant entre parenthèses indique l'augmentation ou la diminution par rapport à la période précédente.
MTTR de l'incident	Ce widget affiche le temps de résolution moyen des incidents de sécurité. Il indique la vitesse à laquelle les incidents font l'objet d'enquêtes et sont résolus. Cliquez sur une colonne pour afficher le détail des incidents en fonction de la gravité (**Critique**, **Élevé** et **Moyen**), ainsi qu'une indication de la durée qui a été nécessaire à la résolution des différents niveaux de gravité. La valeur % figurant entre parenthèses indique l'augmentation ou la diminution par rapport à la période précédente.

Widget	Description
Statut de la menace	Ce widget affiche le statut de menace actuel pour les ressources d'une entreprise (quel que soit le nombre de ressources) en mettant en évidence le nombre actuel d'incidents qui ne sont pas résolus et doivent faire l'objet d'enquêtes. Le widget indique également le nombre d'incidents résolus (manuellement et/ou automatiquement par le système).
Menaces détectées par la technologie de protection	Ce widget affiche le nombre de menaces détectées durant une période spécifique, classées selon les technologies de protection suivantes : • Analyse antimalware • Moteur de comportement • Protection contre le cryptomining • Prévention des failles • Protection active contre les ransomwares • Protection en temps réel • Filtrage d'URL

Widgets de sauvegarde

Le tableau suivant fournit plus de détails sur les widgets de la section **Sauvegarde**.

Widget	Description
Ressources sauvegardées	Ce widget indique le nombre total de ressources enregistrées classées par statut de sauvegarde. **Sauvegardées** : nombre total de ressources sauvegardées (au moins une sauvegarde effectuée avec succès) durant la période couverte par le rapport. **Non sauvegardées** : nombre total de ressources non sauvegardées (aucune sauvegarde effectuée avec succès) durant la période couverte par le rapport.
Intégrité de disque par terminaux physiques	Ce widget affiche les statuts d'intégrité agrégés des terminaux physiques basés sur le statut d'intégrité de leurs disques. **OK** : le statut d'intégrité du disque correspond à une valeur comprise entre [70 à 100]. Le statut du terminal est **OK** quand tous les statuts de ces disques sont **OK**. **Avertissement** : le statut d'intégrité du disque correspond à une valeur comprise entre [30 et 70]. Le statut du terminal est **Avertissement** quand au moins un de ses disques a pour statut **Avertissement**, mais qu'aucun disque n'a pour statut **Erreur**. **Erreur** : le statut d'intégrité du disque correspond à une valeur comprise entre [0 et 30]. Le statut du terminal est **Erreur** quand au moins un de ses disques a pour statut **Erreur**.

Widget	Description
	Calcul des données du disque : le statut du terminal est **Calcul des données du disque** lorsque tous les statuts des disques ne sont pas encore déterminés.
Utilisation du stockage de sauvegarde	Ce widget affiche le nombre total et la taille totale des sauvegardes dans les stockages local et Cloud pour une période spécifiée.

Widgets Évaluation des vulnérabilités et gestion des correctifs

Le tableau suivant fournit plus de détails sur les widgets de la section **Évaluation des vulnérabilités et gestion des correctifs**.

Widget	Description
Vulnérabilités corrigées	Ce widget affiche les résultats de performance du plan d'évaluation de la vulnérabilité pour la période spécifiée. **Total** : le nombre total de vulnérabilités corrigées. **Vulnérabilités logicielles Microsoft** : le nombre total de vulnérabilités Microsoft corrigées sur l'ensemble des terminaux Windows. **Vulnérabilités logicielles tierces Windows** : le nombre total de vulnérabilités tierces corrigées sur l'ensemble des terminaux Windows. **Ressources analysées** : le nombre total de terminaux analysés avec succès à la recherche de vulnérabilités au moins une fois durant la période spécifiée.
Correctifs installés	Ce widget affiche les résultats de performance de gestion des correctifs pour la période spécifiée. **Installés** : le nombre total de correctifs installés avec succès sur l'ensemble des terminaux. **Correctifs logiciels Microsoft** : le nombre total de correctifs logiciels Microsoft installés avec succès sur l'ensemble des terminaux Windows. **Correctifs logiciels tiers Windows** : le nombre total de correctifs logiciels tiers Windows installés avec succès sur l'ensemble des terminaux Windows. **Ressources corrigées** : le nombre total de terminaux corrigés avec succès (au moins un correctif a été installé avec succès durant la période spécifiée).

Widgets de reprise d'activité après sinistre

Le tableau suivant fournit plus de détails sur les widgets de la section **Reprise d'activité après sinistre**.

Widget	Description
Statistiques de reprise d'activité après sinistre	Ce widget affiche les indicateurs de performance clés du plan de reprise d'activité après sinistre pour la période spécifiée. **Basculements de production** : nombre d'opérations de basculement de production pour la période spécifiée. **Basculements de test** : nombre d'opérations de basculement de test effectuées durant la période spécifiée. **Serveurs primaires** : nombre total de serveurs primaires existant au moment de la génération du rapport. **Serveurs de restauration** : nombre total de serveurs de restauration existant au moment de la génération du rapport. **IP publiques** : nombre total d'adresses IP publiques (existant au moment de la génération du rapport). **Total des points de calcul consommés** : nombre total des points de calcul consommés durant la période spécifiée.
Serveurs de reprise d'activité après sinistre testés	Ce widget fournit des informations sur les serveurs protégés par la reprise d'activité après sinistre et vérifiés avec le basculement test. Le widget affiche les indicateurs suivants : **Serveurs protégés** : nombre de serveurs protégés par la reprise d'activité après sinistre (serveurs avec au moins un serveur de restauration) au moment de la génération du rapport. **Testés** : nombre de serveurs protégés par la reprise d'activité après sinistre qui ont été vérifiés avec le basculement test au cours de la période spécifiée, par rapport au nombre total de serveurs protégés par la reprise d'activité après sinistre. **Non testés** : nombre de serveurs protégés par la reprise d'activité après sinistre qui n'ont pas été vérifiés avec le basculement test au cours de la période spécifiée, par rapport au nombre total de serveurs protégés par la reprise d'activité après sinistre. Le widget indique également le volume en Go du stockage de reprise d'activité après sinistre au moment de la génération du rapport. Cela correspond à la somme des volumes de sauvegardes des serveurs Cloud.
Serveurs protégés par la reprise d'activité après sinistre	Ce widget fournit des informations sur les serveurs protégés par la reprise d'activité après sinistre et les serveurs non protégés. Le widget affiche les indicateurs suivants : Le nombre total de serveurs enregistrés dans le tenant client au moment de la génération du rapport. **Protégés** : nombre de serveurs protégés par la reprise d'activité après

Widget	Description
	sinistre (avec au moins un serveur de restauration et une sauvegarde de serveur complète), par rapport au nombre total de serveurs enregistrés au moment de la génération du rapport. **Non protégés** : nombre total de serveurs non protégés, par rapport au le nombre total de serveurs enregistrés au moment de la génération du rapport.

Widget de prévention des pertes de données

Vous trouverez de plus amples informations sur les périphériques bloqués dans la section **Prévention des pertes de données** de la rubrique suivante.

Ce widget indique le nombre total de terminaux bloqués et le nombre total de terminaux bloqués par type de terminaux pour une période spécifique.

- Stockage amovible
- Amovible chiffré
- Imprimantes
- Presse-papiers : inclut les types de terminaux Presse-papiers et Capture d'écran.
- Terminaux mobiles
- Bluetooth
- Lecteurs optiques
- Disquettes
- USB : inclut les types de terminaux Port USB et Port USB redirigé.
- FireWire
- Lecteurs mappés :
- Presse-papiers redirigé : inclut les types de terminaux Presse-papiers redirigé entrant et Presse-papiers redirigé sortant.

Ce widget affiche les sept types de terminaux qui comptabilisent le plus de terminaux bloqués et rassemble les autres types de terminaux sous la classe **Autres**.

Widget File Sync & Share

Le tableau suivant fournit plus de détails sur les widgets de la section **File Sync & Share**.

Widget	Description
Statistiques File Sync & Share	Le widget affiche les indicateurs suivants : **Total de stockage dans le Cloud utilisé** : le total de stockage Cloud utilisé par tous les utilisateurs.

Widget	Description
	Utilisateurs finaux : le nombre total d'utilisateurs finaux. **Moyenne du stockage utilisé par utilisateur final** : le stockage utilisé en moyenne par un utilisateur final. **Utilisateurs invités** : le nombre total d'utilisateurs invités.
Utilisation du stockage File Sync & Share par les utilisateurs finaux	Ce widget indique le nombre total d'utilisateurs File Sync & Share qui utilisent un stockage correspond aux plages suivantes : • 0 à 1 Go • 1 à 5 Go • 5 à 10 Go • 10 à 50 Go • 50 à 100 Go • 100 à 500 Go • 500 Go à 1 To • Plus d'1 To

Widgets de Notary

Le tableau suivant fournit plus de détails sur les widgets de la section **Notary**.

Widget	Description
Statistiques Cyber Notary	Le widget affiche les indicateurs Notary suivants : **Stockage Notary Cloud utilisé** : la taille totale du stockage utilisé pour le service Notary. **Fichiers notarisés** : nombre total de fichiers notarisés. **Documents signés de façon électronique** : le nombre total de documents et fichiers signés de façon électronique.
Fichiers notarisés pour l'ensemble des utilisateurs finaux	Indique le nombre total de fichiers notarisés pour l'ensemble des utilisateurs finaux. Les utilisateurs sont regroupés en fonction de leur nombre de fichiers notarisés. • Jusqu'à 10 fichiers • 11 à 100 fichiers • 101 à 500 fichiers • 501 à 1000 fichiers • Plus de 1 000 fichiers
Documents signés de façon électronique pour l'ensemble des	Ce widget indique le nombre total de documents et fichiers signés de façon électronique pour l'ensemble des utilisateurs finaux. Les utilisateurs sont regroupés en fonction de leur nombre de fichiers et documents signés de façon électronique.

Widget	Description
utilisateurs finaux	• Jusqu'à 10 fichiers • 11 à 100 fichiers • 101 à 500 fichiers • 501 à 1000 fichiers • Plus de 1 000 fichiers

Configuration des paramètres du rapport de synthèse

Vous pouvez modifier les paramètres du rapport de synthèse qui ont été définis lors de sa création.

Pour modifier les paramètres du rapport de synthèse

1. Dans la console de gestion, accédez à **Rapports**>**Synthèse**.
2. Cliquez sur le nom du rapport de synthèse dont vous souhaitez modifier les paramètres.
3. Cliquez sur **Paramètres**.
4. Modifiez les valeurs des champs selon vos besoins.
5. Cliquez sur **Enregistrer**.

Création d'un rapport de synthèse

Pour pouvez créer un rapport de synthèse, visualiser son contenu, configurer ses destinataires et planifier son envoi automatique.

Pour créer un rapport de synthèse

1. Dans la console de gestion, accédez à **Rapports**>**Synthèse**.
2. Cliquez sur **Créer un rapport de synthèse**.
3. Sous **Nom du rapport**, saisissez le nom du rapport.
4. Sélectionnez les destinataires du rapport.
   - Si vous souhaitez envoyer le rapport à tous les contacts et utilisateurs, sélectionnez **Envoyer à tous les contacts et utilisateurs**.
   - Si vous souhaitez envoyer le rapport à des contacts et utilisateurs spécifiques
     a. Désélectionnez **Envoyer à tous les contacts et utilisateurs**.
     b. Cliquez sur **Sélectionner des contacts**.
     c. Sélectionnez les contacts et utilisateurs souhaités. Vous pouvez effectuer une Recherche pour trouver facilement un contact spécifique.
     d. Cliquez sur **Sélectionner**.
5. Sélectionnez une plage : **30 jours** ou **Ce mois-ci**
6. Sélectionnez un format de fichier : **PDF**, **Excel** ou **Excel et PDF**.

7. Configurer les paramètres de planification.
   - Si vous souhaitez envoyer le rapport aux destinataires à une heure et une date spécifiques :
     a. Activez l'option **Planifié**.
     b. Cliquez sur le champ **Jour du mois**, désélectionnez Dernier jour, et cliquez sur le jour souhaité.
     c. Dans le champ **Heure**, saisissez l'heure souhaitée.
     d. Cliquez sur **Appliquer**.
   - Si vous souhaitez créer le rapport sans l'envoyer à ses destinataires, désactivez l'option **Planifié**.
8. Cliquez sur **Enregistrer**.

Personnalisation du rapport de synthèse

Vous pouvez définir les informations à inclure dans le rapport de synthèse. Vous pouvez ajouter ou supprimer des sections, ajouter ou supprimer des widgets, renommer des sections, personnaliser des widgets et glisser-déposer les widgets et sections pour modifier leur ordre d'affichage dans le rapport.

Pour ajouter une section

1. Cliquez sur **Ajouter un élément** > **Ajouter une section**.
2. Dans la fenêtre **Ajouter une section**, saisissez un nom de section, ou utilisez le nom de section par défaut.
3. Cliquez sur **Ajouter au rapport**.

Pour renommer une section

1. Dans la section que vous désirez renommer, cliquez sur **Modifier**.
2. Dans la fenêtre **Modifier la section**, saisissez le nouveau nom.
3. Cliquez sur **Enregistrer**.

Pour supprimer une section

1. Dans la section que vous désirez supprimer, cliquez sur **Supprimer la section**.
2. Dans la fenêtre de confirmation **Supprimer la section**, cliquez sur **Supprimer**.

Pour ajouter un widget avec ses paramètres par défaut à une section

1. Dans la section à laquelle vous souhaitez ajouter le widget, cliquez sur **Ajouter un widget**.
2. Dans la fenêtre **Ajouter un widget**, cliquez sur le widget que vous désirez ajouter.

Pour ajouter un widget personnalisé à une section

1. Dans la section à laquelle vous souhaitez ajouter le widget, cliquez sur **Ajouter un widget**.
2. Dans la fenêtre **Ajouter un widget**, recherchez le widget que vous désirez ajouter, puis cliquez sur **Personnaliser**.
3. Modifiez les champs selon vos besoins.
4. Cliquez sur **Ajouter un widget**.

Pour ajouter un widget avec ses paramètres par défaut au rapport

1. Cliquez sur **Ajouter un élément** > **Ajouter un widget**.
2. Dans la fenêtre **Ajouter un widget**, cliquez sur le widget que vous désirez ajouter.

Pour ajouter un widget personnalisé au rapport

1. Cliquez sur **Ajouter un widget**.
2. Dans la fenêtre **Ajouter un widget**, recherchez le widget que vous désirez ajouter, puis cliquez sur **Personnaliser**.
3. Modifiez les champs selon vos besoins.
4. Cliquez sur **Ajouter un widget**.

Pour rétablir les paramètres par défaut d'un widget

1. Dans le widget que vous désirez personnaliser, cliquez sur **Modifier**.
2. Cliquez sur **Réinitialiser au défaut**.
3. Cliquez sur **Valider**.

Pour personnaliser un widget

1. Dans le widget que vous désirez personnaliser, cliquez sur **Modifier**.
2. Modifiez les champs selon vos besoins.
3. Cliquez sur **Valider**.

Envoi des rapports de synthèse

Vous pouvez envoyer un rapport de synthèse à la demande. Dans ce cas, le paramètre **Planifié** est ignoré, et le rapport est envoyé immédiatement. Pour l'envoi, le système utilise les valeurs de Destinataires, Plage et Format de fichier paramétrées dans les **Paramètres**. Vous pouvez modifier manuellement ces paramètres avant l'envoi du rapport. Pour plus d'informations, voir "Configuration des paramètres du rapport de synthèse" (p. 80).

Pour envoyer un rapport de synthèse

1. Dans le portail de gestion, accédez à **Rapports**>**Synthèse**.
2. Cliquez sur le nom du rapport de synthèse que vous souhaitez envoyer.
3. Cliquez sur **Envoyer maintenant**.
   Le rapport envoie alors le rapport de synthèse aux destinataires sélectionnés.

Fuseaux horaires dans les rapports

Les fuseaux horaires utilisés dans les rapports varient selon le type de rapport. Le tableau suivant contient des informations pour votre information.

Emplacement et type du rapport	Fuseaux horaires utilisés dans le rapport
Portail de gestion > Vue d'ensemble > Opérations (widgets)	L'heure de génération du rapport est indiquée dans le fuseau horaire de la machine sous laquelle le navigateur s'exécute.
Portail de gestion > Vue d'ensemble > Opérations (exporté vers PDF ou xslx)	• L'horodatage du rapport exporté est indiqué dans le fuseau horaire de la machine utilisée pour exporter le rapport. • Le fuseau horaire des activités affichées dans le rapport est indiqué en UTC.
Portail de gestion > Rapports > Utilisation > Rapports planifiés	• Le rapport est généré à 23:59:59 (UTC) le premier jour du mois. • Le rapport est envoyé le deuxième jour du mois.
Portail de gestion > Rapports > Utilisation > Rapports personnalisés	Le fuseau horaire et la date du rapport sont indiqués en UTC.
Portail de gestion > Rapports > Opérations (widgets)	• L'heure de génération du rapport est indiquée dans le fuseau horaire de la machine sous laquelle le navigateur s'exécute. • Le fuseau horaire des activités affichées dans le rapport est indiqué en UTC.
Portail de gestion > Rapports > Opérations (exporté vers PDF ou xslx)	• L'horodatage du rapport exporté est indiqué dans le fuseau horaire de la machine utilisée pour exporter le rapport. • Le fuseau horaire des activités affichées dans le rapport est indiqué en UTC.
Portail de gestion > Rapports > Opérations (livraison planifiée)	• Le fuseau horaire de la livraison du rapport est indiqué en UTC. • Le fuseau horaire des activités affichées dans le rapport est indiqué en UTC.
Portail de gestion > Utilisateurs > Résumé quotidien concernant les alertes actives	• Ce rapport est envoyé une fois entre 10:00 et 23:59 UTC. L'heure à laquelle le rapport est envoyé dépend de la ressource du centre de données. • Le fuseau horaire des activités affichées dans le rapport est indiqué en UTC.
Portail de gestion > Utilisateurs > Notifications du statut de cyberprotection	• Ce rapport est envoyé lorsqu'une activité est terminée. **Remarque** En fonction de la ressource du centre de données, il se peut que certains rapports soient envoyés en retard. • Le fuseau horaire de l'activité du rapport est indiqué en UTC.

Données rapportées en fonction du type de widget

Les widgets du tableau de bord peuvent être classés selon deux catégories, selon le type de données qu'ils présentent :

- Les widgets qui affichent les données actuelles au moment de la navigation ou de la génération du rapport.
- Les widgets qui affichent les données historiques.

Lorsque vous configurez une plage de dates dans les paramètres de rapport afin d'effectuer un vidage mémoire des données d'une certaine période, la plage de dates sélectionnée s'applique uniquement aux widgets qui affichent des données historiques. Elle n'est pas applicable aux widgets qui affichent les données actuelles au moment de la navigation ou de la génération du rapport.

Le tableau suivant énumère les widgets et leurs plages de données.

Nom du widget	Données affichées dans le widget et les rapports
Score #CyberFit par machine	Actuelles
5 dernières alertes	Actuelles
Détails des alertes actives	Actuelles
Résumé des alertes actives	Actuelles
Activités	Historiques
Liste des activités	Historiques
Historique des alertes	Historiques
Analyse anti-malware des sauvegardes	Historiques
Analyse antimalware des fichiers	Historiques
Détails de l'analyse de la sauvegarde (menaces)	Historiques
État de la sauvegarde	Historiques, dans les colonnes **Total des exécutions** et **Nombre d'exécutions réussies** Actuelles, dans toutes les autres colonnes
Utilisation du stockage de sauvegarde	Historiques
Périphériques bloqués	Historiques
URL bloquées	Actuelles
Applications dans le Cloud	Actuelles

Statut de protection des ressources Cloud	Actuelles
Cyberprotection	Actuelles
Résumé Cyber Protection	Historiques
Carte de la protection des données	Historiques
Terminaux	Actuelles
Serveurs de reprise d'activité après sinistre testés	Historiques
Statistiques de reprise d'activité après sinistre	Historiques
Machines découvertes	Actuelles
Vue d'ensemble de l'état de santé du disque	Actuelles
Intégrité du disque	Actuelles
Intégrité de disque par terminaux physiques	Actuelles
Documents signés de façon électronique pour l'ensemble des utilisateurs finaux	Actuelles
Vulnérabilités existantes	Historiques
Statistiques File Sync & Share	Actuelles
Utilisation du stockage File Sync & Share par les utilisateurs finals	Actuelles
Modifications apportées au matériel	Historiques
Détails du matériel	Actuelles
Inventaire matériel	Actuelles
Résumé de l'historique des alertes	Historiques
Résumé des emplacements	Actuelles
Mises à jour manquantes, par catégorie	Actuelles
Non protégé	Actuelles
Fichiers notarisés pour l'ensemble des utilisateurs finaux	Actuelles
Statistiques Notary	Actuelles
Historique d'installation des correctifs	Historiques
Statut d'installation des correctifs	Historiques

Résumé d'installation des correctifs	Historiques
Vulnérabilités corrigées	Historiques
Correctifs installés	Historiques
État de protection	Actuelles
Affectés récemment	Historiques
Sessions distantes	Historiques
Résolution des incidents de sécurité	Historiques
Temps moyen de réparation des incidents de sécurité	Historiques
Serveurs protégés par la reprise d'activité après sinistre	Actuelles
Inventaire du logiciel	Actuelles
Aperçu du logiciel	Historiques
Statut de la menace	Actuelles
Menaces détectées par la technologie de protection	Historiques
Distribution des principaux incidents par ressource	Actuelles
Machines vulnérables	Actuelles
Statut réseau des ressources	Actuelles
Ressources sauvegardées	Historiques
Statut de protection des ressources	Actuelles

Intégrations

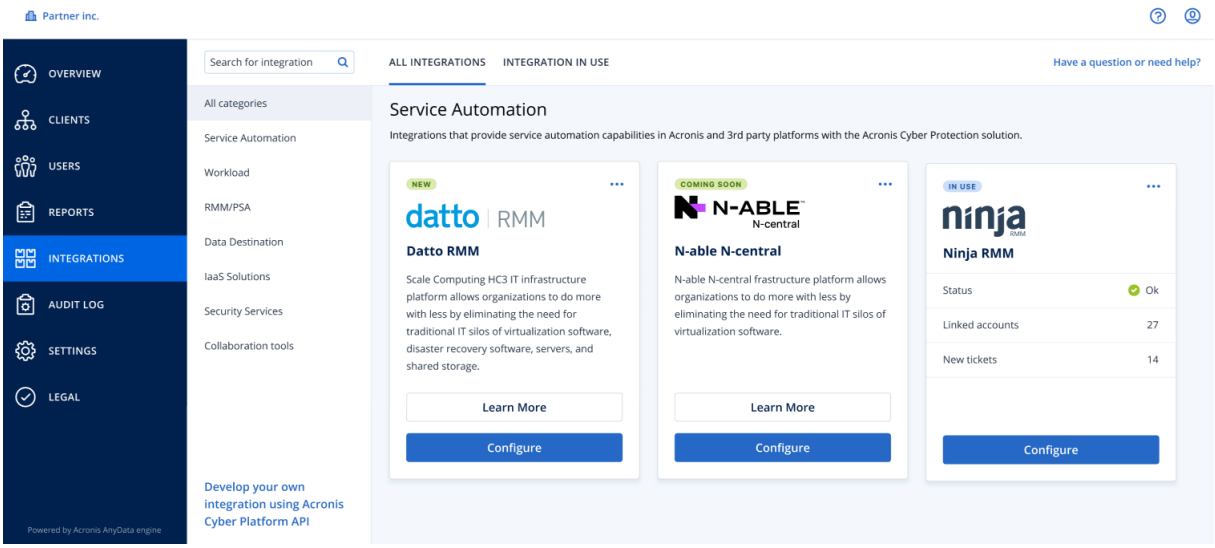
Catalogue des intégrations

Cette page représente l'emplacement global où toutes les applications d'intégration sont enregistrées et mises à jour.
Elle vous permet d'ajouter des intégrations ou de modifier des intégrations existantes.

Remarque
Seuls les utilisateurs ayant un rôle d'**administrateur d'entreprise** sont autorisés à modifier la configuration d'intégration.

Toutes les intégrations

L'onglet **Toutes les intégrations** affiche une liste de toutes les intégrations actuellement disponibles, ordonnées sous forme de vignettes, placées les unes à côté des autres.



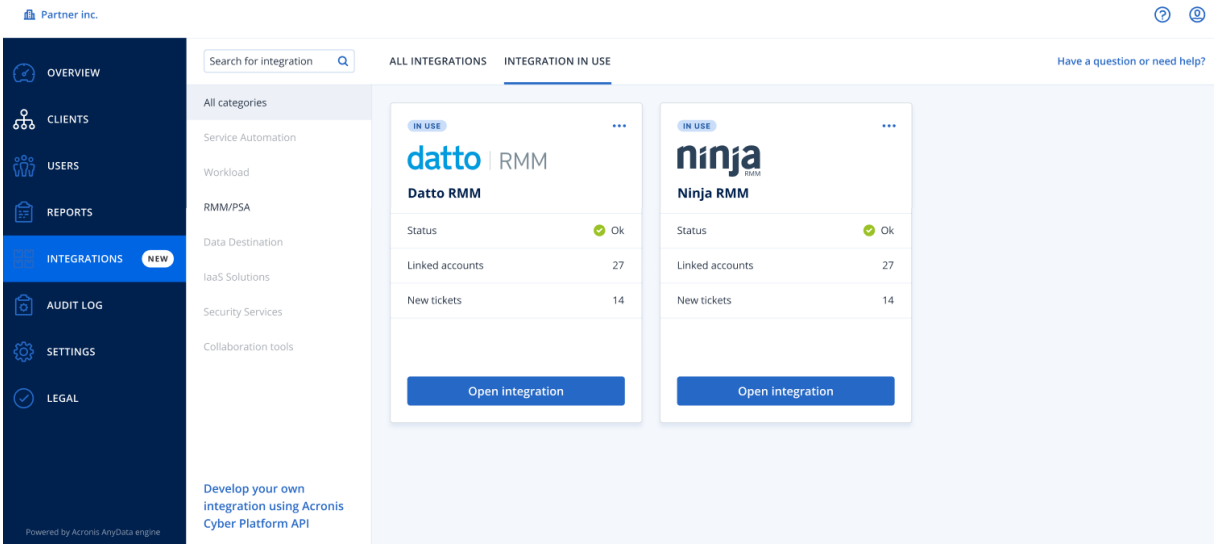
Chaque vignette affiche une courte description du produit et deux options supplémentaires :

- **En savoir plus** - Cliquez sur ce bouton pour obtenir plus d'informations sur l'intégration concernée :
  - **Fonctionnalités de l'intégration**
  - **Liens vers la documentation**
  - **Contacts de support**
- **Configurer** - Cette option vous permet de modifier certains des paramètres de l'intégration.

Les vignettes qui représentent des intégrations inactives apparaissent grisées et sont désactivées. Elles peuvent aussi porter la mention « **Bientôt disponible** ».

Intégrations utilisées

L'onglet **Intégrations utilisées** affiche une liste de toutes les intégrations qui sont actuellement utilisées. Chacune d'entre elles est accompagnée d'informations générales.



Cliquez sur **Ouvrir l'intégration** pour accéder directement à l'application correspondante.

Sur la gauche, vous trouverez une liste des catégories d'intégration, dans lesquelles toutes les applications existantes sont classées dans différents groupes, par exemple automatisation de service, ressource, RMM/PSA, etc. Cliquez sur chaque catégorie individuelle pour afficher les intégrations qui appartiennent à ce groupe particulier. La catégorie que vous consultez actuellement est mise en surbrillance.

L'option **Rechercher** vous permet d'effectuer des requêtes et de rechercher les intégrations de votre choix.

Vous pouvez filtrer la liste des intégrations par catégorie ou libellé. Les libellés sont classés par ordre alphabétique. Si la recherche ne donne aucun résultat, élargissez-la à d'autres catégories.

Pour désactiver une application, cliquez sur l'icône en forme de points de suspension (...) dans l'angle supérieur droit, puis sélectionnez **Désactiver**.

Un lien vers la document de l'API Acronis est également disponible, si le développement de votre propre intégration vous intéresse.

Limitation de l'accès à l'interface Web

Vous pouvez limiter l'accès à l'interface Web en spécifiant une liste d'adresses IP à partir desquelles les utilisateurs sont autorisés à se connecter.

Cette restriction s'applique également à l'accès au portail de gestion via l'API.

Cette restriction s'applique uniquement au niveau où elle est paramétrée. Elle ne s'applique *pas* aux membres des unités enfants.

Pour limiter l'accès à l'interface Web

1. Connectez-vous au portail de gestion.
2. Naviguez vers l'unité à laquelle vous souhaitez limiter l'accès.
3. Cliquez sur **Paramètres** > **Sécurité**.
4. Sélectionnez la case à cocher **Activer le contrôle de connexion**.
5. Dans **Adresses IP autorisées**, spécifiez les adresses IP autorisées.
   Vous pouvez saisir n'importe quels paramètres suivants, séparés par des points virgules :
   - Des adresses IP, par exemple : 192.0.2.0
   - Des plages IP, par exemple : 192.0.2.0-192.0.2.255
   - Des sous-réseaux, par exemple : 192.0.2.0/24
6. Cliquez sur **Enregistrer**.

Limitez l'accès à votre société

Les administrateurs de sociétés peuvent limiter l'accès des gestionnaires de niveau supérieur à leur société.

Si l'accès à la société est limité, les administrateurs de niveau supérieur peuvent modifier uniquement les propriétés de la société. Ils n'ont plus du tout accès aux comptes utilisateur ni aux unités enfants.

Pour limiter l'accès à la société

1. Connectez-vous au portail de gestion.
2. Cliquez sur **Paramètres** > **Sécurité**.
3. Désactivez l'option **Accès à l'assistance**.
4. Cliquez sur **Enregistrer**.

Gestion des clients d'API

Des systèmes tiers peuvent être intégrés à Cyber Protect Cloud en utilisant ses interfaces de programmation d'application (API). L'accès à ces API est fourni par des clients d'API, qui font partie intégrante de l'infrastructure d'autorisation OAuth 2.0 de la plate-forme.

Qu'est-ce qu'un client d'API ?

Un client d'API est un compte de plate-forme spécial dont le but est de représenter un système tiers nécessitant de s'authentifier et d'être autorisé à accéder à des données dans les API des plates-formes et de ses services.

L'accès du client est limité à un tenant, dans lequel l'administrateur crée le client, et à ses sous-tenants.

Lors de sa création, le client hérite des rôles de service du compte administrateur, et ces rôles ne peuvent pas être modifiés ultérieurement. Modifier les rôles d'un compte administrateur ou le désactiver n'affecte pas le client.

Les identifiants du client consistent en un identificateur unique (ID) et une valeur de code secret. Les identifiants n'expirent pas et ne peuvent pas servir à se connecter au portail de gestion ou à une console de service. La valeur du code secret peut être réinitialisée.

Il est impossible d'activer l'authentification à deux facteurs pour le client.

Procédure d'installation typique

1. Un administrateur crée un client d'API dans le tenant, qu'un système tiers gèrera.
2. L'administrateur active le flux d'identifiants du client OAuth 2.0 dans le système tiers.
   En fonction de ce flux, avant d'accéder au tenant et à ses services via l'API, le système doit d'abord envoyer les identifiants du client créé à la plate-forme à l'aide de l'API d'autorisation. La plate-forme génère et envoie un jeton de sécurité, c'est-à-dire la chaîne chiffrée unique attribuée à ce client en particulier. Le système doit ensuite ajouter ce jeton à toutes les demandes d'API.
   Un jeton de sécurité élimine le besoin de passer par des demandes d'API pour obtenir les identifiants du client. Pour plus de sécurité, le jeton expire au bout de deux heures. Une fois ce délai écoulé, toutes les demandes d'API effectuées avec le jeton expiré échoueront, et le système devra demander un nouveau jeton à la plate-forme.

Pour plus d'informations à propos de l'utilisation des API d'autorisation et de plate-forme, reportez-vous au guide du développeur à l'adresse https://developer.acronis.com/doc/account-management/v2/guide/index.

Création d'un client d'API

1. Connectez-vous au portail de gestion.
2. Cliquez sur **Paramètres** > **Clients d'API** > **Créer un client d'API**.
3. Saisissez un nom pour le client d'API.
4. Cliquez sur **Suivant**.
   Le client d'API est créé avec l'état **Activé** par défaut.
5. Copiez et enregistrez l'ID et le code secret du client, ainsi que l'URL du centre de données. Vous en aurez besoin pour activer le flux d'identifiant du client OAuth 2.0 dans un système tiers.

   Important
   Pour des raisons de sécurité, la valeur du code secret ne s'affiche qu'une seule fois. Il n'existe aucun moyen de récupérer cette valeur si vous la perdez, vous serez obligé de la réinitialiser.

6. Cliquez sur **Valider**.

Réinitialiser la valeur du code secret d'un client d'API

1. Connectez-vous au portail de gestion.
2. Cliquez sur **Paramètres** > **Clients de l'API**.
3. Trouvez le client requis dans la liste.
4. Cliquez sur , puis cliquez sur **Réinitialiser le code secret**.
5. Confirmez votre choix en cliquant sur **Suivant**.
   Un nouveau code secret sera généré. L'ID du client et l'URL du centre de données ne changeront pas.
   Tous les jetons de sécurité attribués à ce client expireront immédiatement et les demandes d'API pour ces jetons échoueront.
6. Copiez et enregistrez la valeur du nouveau code secret du client.

   Important
   Pour des raisons de sécurité, la valeur du code secret ne s'affiche qu'une seule fois. Il n'existe aucun moyen de récupérer cette valeur si vous la perdez, vous serez obligé de la réinitialiser.
7. Cliquez sur **Valider**.

Désactiver un client d'API

1. Connectez-vous au portail de gestion.
2. Cliquez sur **Paramètres** > **Clients de l'API**.
3. Trouvez le client requis dans la liste.
4. Cliquez sur , puis sur **Désactiver**.
5. Confirmez votre choix.
   L'état du client changera pour **Désactivé**.
   Toutes les demandes effectuées avec des jetons de sécurité attribués à ce client échoueront, mais les jetons n'expireront pas immédiatement. Désactiver le client n'affecte pas le délai d'expiration des jetons.
   Il sera possible de réactiver le client à tout moment.

Activation d'un client d'API désactivé

1. Connectez-vous au portail de gestion.
2. Cliquez sur **Paramètres** > **Clients de l'API**.
3. Trouvez le client requis dans la liste.
4. Cliquez sur , puis sur **Activer**.

L'état du client changera pour **Activé**.

Les demandes effectuées avec des jetons de sécurité attribués à ce client réussiront si ces jetons n'ont pas encore expiré.

Suppression d'un client d'API

1. Connectez-vous au portail de gestion.
2. Cliquez sur **Paramètres** > **Clients de l'API**.
3. Trouvez le client requis dans la liste.
4. Cliquez sur , puis sur **Supprimer**.
5. Confirmez votre choix.

   Tous les jetons de sécurité attribués à ce client expireront immédiatement et les demandes d'API pour ces jetons échoueront.

Important

Il est impossible de restaurer un client supprimé.

Index