chrome enterprise

Guide de configuration **Chrome Enterprise Premium**

Avril 2024

chrome enterprise

Sommaire

chrome enterprise

Vue d'ensemble de Chrome Enterprise Premium

La navigation d'entreprise sécurisée est la norme émergente pour protéger les données de l'entreprise tout en permettant aux utilisateurs de travailler en toute sécurité sur le Web, où qu'ils se trouvent et quel que soit l'appareil utilisé. Chrome Enterprise Premium offre les avantages suivants :

- Une protection robuste contre la perte de données
  - Des commandes personnalisables pour protéger les informations sensibles
- Une défense proactive contre les menaces
  - Une protection en temps réel contre l'hameçonnage, les logiciels malveillants et les menaces isolées
- Une gestion précise des accès
  - Un accès limité aux applications essentielles selon le principe du moindre privilège

Ce guide fournit les étapes à suivre pour configurer Chrome Enterprise Premium en vue d'une gestion basée sur les utilisateurs ou sur les appareils (ou les deux). Il présente également les étapes à suivre pour configurer une version d'essai (si nécessaire) et pour activer les insights sur la sécurité des données dans Chrome afin d'effectuer un examen sans frais de la sécurité des activités de navigation potentiellement risquées dans votre entreprise.

Conditions requises :

- Navigateur Chrome installé sur les appareils des utilisateurs
- Une licence Chrome Enterprise Premium
- Accès à une console d'administration Google
- Accès à une console Google Cloud
- L'enregistrement des appareils dans la gestion cloud du navigateur Chrome et/ou l'achat de licences Google Cloud Identity afin de gérer les utilisateurs

chrome enterprise

Cas d'utilisation traités dans ce guide

Chrome Enterprise Premium offre un large éventail de fonctionnalités qui couvrent de nombreux cas d'utilisation courants pour les entreprises.

Ce guide aborde les commandes les plus courantes et les plus efficaces que vous pouvez appliquer rapidement :

1. Limiter les risques internes et les risques d'exfiltration de données provenant de l'entreprise et de partenaires tiers
2. Gérer l'accès et la sécurité pour les applications et les ressources sur des appareils gérés et non gérés
3. Simplifier et réduire votre empreinte VDI en fournissant un accès sécurisé aux applications essentielles

chrome enterprise

Gestion basée sur l'utilisateur ou sur l'appareil

Choisir la solution adaptée à votre cas d'utilisation

Chrome Enterprise Premium fournit une assistance pour l'application de règles basées sur l'utilisateur et sur l'appareil.
Remarque : si vous le souhaitez, vous pouvez appliquer à la fois une gestion basée sur l'utilisateur et sur l'appareil.
Pour en savoir plus sur la gestion basée sur l'utilisateur ou sur l'appareil, consultez cet article du Centre d'aide.

Voici un aperçu des fonctionnalités compatibles avec ces deux types de gestion :

		Gestion basée sur l'utilisateur	Gestion basée sur l'appareil
Compatibilité avec les machines non gérées	Possibilité d'appliquer des règles et des mesures de sécurisation du navigateur aux appareils non fournis par l'entreprise	✓	
Application de règles obligatoires au niveau de l'appareil	Possibilité d'appliquer des règles et des mesures de sécurisation du navigateur à tous les profils utilisateur sans que les utilisateurs n'aient à se connecter à Chrome		✓
Synchronisation des données Chrome entre plusieurs machines	Possibilité de déplacer les données Chrome (comme l'historique et les favoris) d'une machine à une autre si l'utilisateur se connecte	✓	
Intégrations Chrome	Connecteurs Chrome Intégrations avec les fournisseurs d'identité (par exemple, Okta, Ping, etc.), envoi de rapports sur les événements liés à la sécurité aux outils SIEM (par exemple, Chronicle, Splunk, etc.)	✓	✓
Insights sur la sécurité des données dans Chrome	Rapports liés aux insights sur la sécurité des données dans Chrome	✓	✓
Sécurité Chrome avancée	Détection approfondie des logiciels malveillants	✓	✓
	Classification et filtrage des URL	✓	✓
	Détection de l'hameçonnage en temps réel	✓	✓
	Protection contre la perte de données (y compris des fonctionnalités d'accès contextuel)	✓	✓
	Evidence Locker (enregistrement du contenu lorsqu'une règle de protection des données est déclenchée en vue d'un examen)	✓	✓
	Accès contextuel aux applications SaaS et aux applications Web privées via Chrome	✓	✓

chrome enterprise

Premiers pas

Options d'accès pour Chrome Enterprise Premium

Pour configurer une gestion du navigateur Chrome basée sur l'utilisateur ou sur l'appareil, vous devez disposer d'un accès à une console d'administration Google et à une console Google Cloud. Il existe deux options pour accéder à la console d'administration :

Option 1 : Vous ne disposez pas encore d'une console d'administration Google ?

- Cliquez sur ce lien pour configurer votre compte, puis suivez les étapes pour valider votre domaine.
- Un accès à une console Google Cloud sera également fourni durant ce processus. Lors de leur connexion à la console Cloud, les utilisateurs sont invités à accepter les conditions d'utilisation de GCP.
- La console est fournie sans coût supplémentaire.

Option 2 : Vous disposez déjà d'une console d'administration Google ?

- Si la console est déjà configurée, la gestion cloud du navigateur Chrome est déjà disponible. Il vous suffit de l'activer. Suivez ces étapes pour l'ajouter à vos abonnements sans coût supplémentaire.
- Une console Google Cloud est également déjà configurée.

La meilleure solution est d'utiliser la console d'administration Google existante de votre entreprise, le cas échéant. Vous devrez contacter votre super-administrateur pour obtenir les droits nécessaires afin de gérer les règles Chrome et de configurer les commandes de sécurité Chrome Enterprise Premium. Pour en savoir plus, reportez-vous à la page suivante.

chrome enterprise

Premiers pas

Configurer des rôles d'administrateur dans la console d'administration Google

Privilèges requis dans la console d'administration Google

Un rôle personnalisé devra être créé dans la console d'administration Google. Pour créer des rôles personnalisés, il faut un compte super-administrateur.

1. Accédez à Compte > Rôles d'administrateur.
2. Cliquez sur le bouton "Créer un rôle" et donnez-lui un nom, par exemple "Administrateur Chrome Enterprise Premium". Ensuite, cliquez sur le bouton "Continuer".
3. Sélectionnez les privilèges suivants dans la console d'administration :

Console d'administration Google	
Unités organisationnelles	Cochez "Lire", "Créer" et "Mettre à jour" (l'option "Supprimer" est facultative, mais recommandée).
Gestion de Chrome	Cochez "Paramètres" pour accorder tous les droits de gestion de Chrome.
Centre de sécurité	Cochez "Cet utilisateur dispose des droits d'administrateur complets pour le centre de sécurité".
Sécurité des données	Cochez "Gestion des niveaux d'accès" et "Gestion des règles".
Centre d'alerte	Cochez "Accès complet".
Protection contre la perte de données Chrome	Cochez "Gérer les paramètres des insights sur l'application de la Protection contre la perte de données dans Chrome" et "Afficher les paramètres des insights sur l'application de la Protection contre la perte de données dans Chrome".
Protection contre la perte de données	Cochez la case.
Chrome Enterprise Premium	Cochez la case.
Rapports	Cochez la case.

4. Une fois les options ci-dessus sélectionnées, cliquez sur le bouton "Continuer".
5. Cliquez sur le bouton "Créer un rôle".
6. Sélectionnez le rôle personnalisé que vous avez créé lors de l'étape précédente, puis cliquez sur le bouton "Attribuer un rôle" pour l'attribuer aux administrateurs sélectionnés.

chrome enterprise

Premiers pas

Configurer des rôles d'administrateur dans la console Google Cloud

Privilèges requis dans la console Google Cloud

Un rôle personnalisé devra être créé dans la console Google Cloud. Pour créer des rôles personnalisés, vous devez disposer de privilèges suffisants.

1. Accédez à Principale > IAM et administration > Rôles et cliquez sur "CRÉER UN RÔLE" pour créer un rôle au niveau de l'organisation et lui donner un nom, par exemple "Administrateur Chrome Enterprise Premium".

   Pour activer la licence Chrome Enterprise Premium et les configurations supplémentaires, vous devez accorder les droits suivants :

Console Google Cloud (définir au niveau de l'organisation)
Rôle de lecteur GCP (définir au niveau de l'organisation et du projet afin de voir les ressources et les projets)
Rôle d'administrateur cloud BeyondCorp (définir au niveau de l'organisation et du projet)
Rôle d'administrateur des abonnements cloud BeyondCorp (définir au niveau de l'organisation)

   Vous devrez également sélectionner les autorisations sur plusieurs pages :

2. Cliquez sur "CRÉER" pour terminer.
3. Accédez à Principale > IAM et administration > IAM et cliquez sur "AJOUTER" pour ajouter un administrateur.
   - Assurez-vous d'effectuer cette action au niveau de l'ORGANISATION.
4. Sélectionnez votre administrateur dans la zone des nouveaux membres.
5. Sélectionnez le rôle Personnalisé > Administrateur Chrome Enterprise Premium.
6. Cliquez sur "ENREGISTRER" pour terminer.
7. Sur le même écran, sélectionnez le projet que vous souhaitez utiliser à des fins de test.
8. Cliquez sur "AJOUTER" pour ajouter des autorisations pour l'administrateur.
9. Sélectionnez votre administrateur dans la zone des nouveaux membres.
10. Cliquez sur "De base", puis sélectionnez le rôle "Propriétaire".
11. Cliquez sur "ENREGISTRER" pour terminer.

chrome enterprise

Configurer des utilisateurs et/ou des appareils gérés

Gérer les règles Chrome dans la console d'administration

Les commandes avancées de protection des données et de défense contre les menaces de Chrome Enterprise Premium sont activées par des règles définies dans la console d'administration Google. Pour appliquer ces règles, vous devrez soit créer des comptes utilisateur gérés, soit enregistrer des appareils dans la console. Les règles cloud de Chrome peuvent s'appliquer au niveau de l'utilisateur connecté ou de la machine, et peuvent offrir différents types de protections et de visibilité. Il est recommandé d'utiliser la gestion basée sur l'appareil pour les appareils gérés par l'entreprise, et d'utiliser la gestion basée sur l'utilisateur pour le personnel élargi. Pour en savoir plus sur la différence entre ces deux modes de gestion, reportez-vous au tableau ci-dessous :

Champ d'application des règles cloud	Utilisateur (profil)	Machine (appareil)
Cas d'utilisation typique	• Appareils non gérés/appareils fournis par le sous-traitant • Utilisateurs professionnels utilisant leur propre appareil	Appareil détenu par l'entreprise
Application des règles	Lors de la connexion de l'utilisateur à Chrome	Aucune connexion (ni identification) requise
Application des règles au niveau de l'appareil	Appliquées au niveau de chaque utilisateur	Appliquées à tous les profils Chrome
Exigences concernant les licences	Licences utilisateur Google Identity ou Google Workspace	Aucune
Configuration de l'administrateur	Configurer des règles dans le navigateur Chrome	• Générer et déployer un jeton d'inscription vers les appareils à l'aide d'une règle au niveau du système d'exploitation (par exemple, GPO) • Configurer des règles dans le navigateur Chrome
Précision des rapports sur les événements liés à la sécurité	Rapports sur l'activité des utilisateurs connectés	Rapports au niveau de l'appareil pour tous les profils. Les informations sur l'utilisateur ne sont pas enregistrées.
Rapports sur le navigateur Chrome (extension, version)	Actuellement non disponibles au niveau du profil	Disponibles en tant que rapports sur l'appareil pour tous les profils

Avant de passer aux étapes suivantes, vous devrez enregistrer des navigateurs dans la gestion cloud du navigateur Chrome et/ou créer des comptes utilisateur Google gérés. Voici comment procéder dans chaque cas (gestion basée sur l'appareil ou sur l'utilisateur) :

- **Gestion basée sur l'utilisateur** : article du Centre d'aide sur la configuration du profil utilisateur cloud Chrome
- **Gestion basée sur l'appareil** : article du Centre d'aide ou guide de configuration dans la console d'administration concernant les machines (appareils) cloud Chrome

REMARQUES

- Si vous gérez actuellement les règles Chrome au niveau du système d'exploitation (par exemple, GPO pour Windows), les règles cloud Chrome peuvent coexister. Il n'est pas nécessaire de modifier les processus existants concernant les règles Chrome pour activer les règles Chrome Enterprise Premium dans la console d'administration.
- En cas de conflit de règles, Chrome adhère à une priorité des règles par défaut. Il existe des règles permettant de fusionner les règles ou d'ignorer l'ordre de priorité par défaut.

chrome enterprise

Démarrer un essai de Chrome Enterprise Premium

Activer un essai dans votre console Google Cloud

1. Accédez à la console Google Cloud.
2. Recherchez “Chrome Enterprise Premium”.
3. Cliquez sur "S'inscrire", puis sur "Commencer l'essai gratuit" pour activer l'essai.
4. Sélectionnez le projet auquel vous voulez appliquer l'essai.
5. Votre essai de 30 jours est à présent activé. Veuillez attendre environ cinq minutes que l'opération se termine.
6. Vous pouvez consulter le lien suivant concernant l'attribution de licences Chrome Enterprise Premium aux utilisateurs pour savoir comment appliquer votre essai aux comptes utilisateur ou aux appareils dans la console d'administration Google.
7. Avant de passer à l'étape suivante, vous devez attribuer une licence à l'administrateur ainsi qu'aux appareils/comptes utilisateur. Pour ce faire, accédez à Facturation > Paramètres de licence > Attribuer des licences. Vous pouvez également attribuer des licences automatiquement en suivant ces étapes.

Activer les insights sur la sécurité des données dans Chrome

Une fois que vous avez activé l'essai et configuré vos comptes administrateur, vous pouvez activer les insights sur la sécurité des données dans Chrome afin de procéder à un examen de la sécurité de votre environnement. Cet examen sans frais vous offre les avantages suivants :

- Vous pouvez analyser les activités internes à haut risque ainsi que les tentatives d'exfiltration de données.
- Les utilisateurs finaux ne subissent aucune perturbation.
- Vous pouvez créer des rapports qui vous guideront dans les mesures à prendre pour sécuriser davantage vos données dans le navigateur.

Pour configurer ces fonctionnalités, procédez comme suit :

1. Accédez à admin.google.com et cliquez sur l'onglet de la page d'accueil à gauche.
2. L'option "Surveillez les fuites de données et les risques internes" s'affichera en haut à droite.
    - Assurez-vous de disposer de droits de super-administrateur, nécessaires pour activer cette fonctionnalité.
3. Cliquez sur le bouton "Activer" au bas de la fenêtre pop-up.

À ce stade, vous voudrez sans doute permettre à Chrome de collecter les détails concernant les actions et les activités des utilisateurs au cours de la semaine ou des deux semaines qui suivent afin d'obtenir un meilleur aperçu de votre consommation de données et des menaces potentielles. Pour plus d'informations sur cette fonctionnalité, consultez cet article du Centre d'aide.

Une fois le processus de collecte terminé, vous obtiendrez plusieurs rapports qui pourront être consultés pour une meilleure compréhension et une plus grande visibilité. Notez que si vous avez déjà activé les connecteurs Chrome Enterprise, les insights sur la sécurité Chrome ne seront pas activés et votre configuration restera en l'état.

Ces rapports vous aideront à déterminer les domaines sensibles qui pourraient nécessiter une attention supplémentaire et des contrôles de sécurité multicouches. Vous les trouverez dans les tableaux de bord du centre de sécurité, à gauche de la console d'administration.

chrome enterprise

Cas d'utilisation de Chrome Enterprise Premium

La plupart des cas d'utilisation de Chrome Enterprise Premium reposent sur une configuration similaire. Selon que vous prenez en charge des appareils/utilisateurs gérés ou non gérés, les paramètres peuvent varier.

Les cas d'utilisation suivants fournissent un ensemble de paramètres généraux qui peuvent être appliqués avec Chrome Enterprise Premium.

Cas d'utilisation n° 1 : limiter les risques internes et les risques d'exfiltration de données

Définir des règles de protection contre la perte de données dans la console d'administration

Une fois que vous avez examiné les résultats du rapport relatif aux insights sur la sécurité Chrome des étapes précédentes, vous pouvez commencer à définir des règles pour protéger vos ressources les plus sensibles. Pour démarrer, consultez les liens suivants :

- Activer les paramètres Chrome Enterprise Premium dans la console d'administration Google
- Activer les règles de protection contre la perte de données dans la console d'administration Google
- Gérer la validation des points de terminaison pour les appareils gérés
- Protéger les données à l'aide de l'accès contextuel
- Combiner les règles de protection contre la perte de données avec des conditions d'accès contextuel

Obtenir une visibilité approfondie grâce aux événements liés à la sécurité

La visibilité des activités dangereuses réalisées par les utilisateurs est l'un des aspects les plus critiques des programmes de sécurité. La solution de protection des données et de prévention des menaces Chrome Enterprise Premium capture des événements de journal détaillés pour les activités risquées des utilisateurs afin que les administrateurs puissent surveiller, examiner et analyser les activités et les comportements des utilisateurs, puis limiter les risques au sein de leur organisation. Pour en savoir plus sur l'affichage et l'audit de ces informations, veuillez consulter les liens suivants.

- Comprendre et réaliser un audit des différents événements liés à la sécurité dans la console d'administration Google
- Utiliser le connecteur de création de rapports de Chrome pour envoyer les événements liés à la sécurité à votre outil SIEM
- Utiliser le tableau de bord de sécurité dans la console d'administration Google
- Utiliser l'outil d'investigation de sécurité pour inspecter les événements liés à la sécurité et y remédier

chrome enterprise

Cas d'utilisation de Chrome Enterprise Premium

Cas d'utilisation n° 2 : gérer l'accès et la sécurité pour les employés utilisant des appareils non gérés

Configurer un accès contextuel

La prise en charge des utilisateurs distants ou sous-traitants peut s'avérer difficile lorsque vous n'avez pas la possibilité de transférer des agents classiques sur les machines non gérées. Avec Chrome et Chrome Enterprise Premium, vous pouvez appliquer des niveaux d'accès aux applications critiques grâce à une solution sans agent qui empêche le téléchargement, l'enregistrement, la copie ou l'impression d'informations sensibles de l'entreprise.

Pour démarrer, consultez les liens suivants :

- Activer les paramètres Chrome Enterprise Premium dans la console d'administration Google
- Activer les règles de protection contre la perte de données dans la console d'administration Google
- Combiner les règles de protection contre la perte de données avec des conditions d'accès contextuel

Intégrer Chrome à votre fournisseur d'identité à l'aide d'un connecteur de confiance des appareils

Les connecteurs de confiance des appareils Chrome Enterprise partagent les signaux contextuels provenant des appareils ChromeOS et des navigateurs Chrome gérés avec les fournisseurs d'identité tiers. Cette intégration permet aux signaux de confiance des appareils d'être pris en compte dans les règles d'authentification et d'autorisation.

- Gérer les connecteurs de confiance des appareils Chrome Enterprise dans la console d'administration Google

Protéger les applications Web privées à l'aide de Chrome Enterprise Premium

Les applications Web privées sont créées pour les utilisateurs internes d'une organisation, comme les employés et les sous-traitants. Ces applications peuvent être déployées à l'aide de Chrome Enterprise Premium dans la console d'administration Google. De plus, elles sont compatibles avec les applications hébergées dans Google Cloud ou dans d'autres clouds et centres de données sur site.

Pour démarrer, consultez les liens suivants :

- Ajouter l'application à votre compte Workspace
- Paramètres pour les applications hébergées sur Google Cloud
- Paramètres pour les applications hébergées par d'autres fournisseurs de services cloud ou dans des centres de données sur site
- Restreindre l'accès et l'authentification

Cas d'utilisation de Chrome Enterprise Premium

Cas d'utilisation n° 3 : simplifier et réduire votre empreinte VDI

Configurer un accès contextuel

Les anciennes solutions VDI peuvent être coûteuses, compliquées à mettre en place et difficiles à sécuriser et à utiliser. Grâce à Chrome Enterprise Premium, vous pouvez permettre aux utilisateurs d'accéder directement et en toute sécurité à des applications Web privées comme s'il s'agissait d'une application SaaS.

Pour remplacer la VDI, les clients utilisent désormais des technologies telles que la diffusion d'applications en continu pour fournir des applications sécurisées pouvant être intégrées aux fonctionnalités de sécurité de Chrome Enterprise Premium. Ils obtiennent ainsi une solution de conteneurs sécurisée complète.

Cas d'utilisation n° 4 : contrôler l'accès au shadow IT grâce à une plus grande visibilité

Empêcher les utilisateurs d'accéder à des applications Web risquées et stopper l'exfiltration des données

Qu'elles soient accidentelles ou malveillantes, certaines actions des utilisateurs peuvent mettre en péril les données de l'entreprise en les stockant dans des SaaS peu sécurisés. En activant Chrome Enterprise Premium, vous pouvez :

- exploiter le filtrage des URL pour bloquer les applications SaaS risquées non approuvées et empêcher les utilisateurs de visiter des sites Web non sécurisés ;
- activer des règles de protection des données pour bloquer les transferts de fichiers (téléchargement, chargement, enregistrement, copie, impression) sur les appareils non gérés et avertir les utilisateurs du transfert de données sensibles sur les appareils gérés ;
- activer les connecteurs de confiance des appareils Chrome pour fournir une authentification transparente sans qu'il soit nécessaire de modifier les flux SAML.

Pour démarrer, consultez les liens suivants :

- Exemples de règles de navigation vers des URL
- Bloquer la navigation Chrome vers une liste d'URL personnalisée
- Connecteurs de confiance des appareils Chrome

chrome enterprise

Résolution des problèmes liés aux fonctionnalités de protection des données

Résolution des problèmes côté navigateur

Cette section fournit des conseils sur la résolution des problèmes liés aux fonctionnalités de protection des données et de prévention des menaces. La plupart des écrans de débogage se trouvent sur la page chrome://safe-browsing, par exemple :

chrome://safe-browsing/#tab-urt-lookup

Cet onglet présente tous les événements d'analyse d'URL et leurs résultats.

Vous trouverez ci-dessous un exemple de vérification de l'URL en temps réel lorsque vous essayez de télécharger un fichier CSV sûr.


```
{
  "dm_token": "ABjmT7kMHtEiDhVFYvEAXO_xdM0C-tIZwZTe3-bbdpMuzAvQCN5U2jKULX40pxJ
iqURvuhYXBphcKwgW-AmLyGRsIwexkmyPtCpKyEtjjiLOiBqrb7G7UMl1_JqXshV5DEAYb2_pZFTAI
a2HY5TRrIZfDPqCZYRnbde9ovSX0d5zDWzUczeRtqEnHvxBgq3ptDyensyP4oHatZv3AfhyPvY9I
YDU-2Ay5q2ScaKsbklu6u007vv6HC8=",
  "lookup_type": "NAVIGATION",
  "os": "LINUX",
  "population": {
    "finch_active_groups": [  ],
    "is_history_sync_enabled": true,
    "is_incognito": false,
    "is_under_advanced_protection": false,
    "profile_management_status": "UNAVAILABLE",
    "user_population": "EXTENDED_REPORTING"
  },
  "scoped_oauth_token": "",
  "url": "https://dlptest.com/sample-data.csv",
  "version": 1
}
```

```
{
  "threat_infos": [ {
    "cache_duration_sec": 300.0,
    "cache_expression": "dlptest.com/sample-data.csv",
    "cache_expression_match_type": "EXACT_MATCH",
    "cache_expression_using_match_type": "dlptest.com/sample-data.csv",
    "threat_type": "THREAT_TYPE_UNSPECIFIED",
    "verdict_type": "SAFE"
  } ]
}
```


chrome://safe-browsing/#tab-deep-scan

Cet onglet présente tous les événements d'analyse de contenu (logiciels malveillants, protection contre la perte de données) et les résultats obtenus.

Vous trouverez ci-dessous un exemple de vérification des logiciels malveillants et de la protection contre la perte de données pour le fichier CSV.

- CSV n'est pas un type de fichier compatible avec la vérification des logiciels malveillants, de sorte qu'aucune règle ne devrait être déclenchée.
- On voit toutefois que la règle de protection contre la perte de données est déclenchée.


```
[5/1/2021, 3:55:22 AM]
{
  "analysis_connector": "FILE_DOWNLOADED",
  "device_token": "ABjmT7kMHtEiDhVFYvEAXO_xdM0C-tIZwZTe3-bbdpMuzAvQCN5U2jKULX40p
xJiqURvuhYXBphcKwgW-AmLyGRsIwexkmyPtCpKyEtjjiLOiBqrb7G7UMl1_JqXshV5DEAYb2_pZFTA
Ia2HY5TRrIZfDPqCZYRnbde9ovSX0d5zDWzUczeRtqEnHvxBgq3ptDyensyP4oHatZv3AfhyPvY9IY
DU-2Ay5q2ScaKsbklu6u007vv6HC8=",
  "fcm_notification_token": "d1Rhf-6b4gU:APA91bHV9udlssAr2Yx2SEJHxmdwSMgEzPYV8EpbaC
JBthYnEpFsujKftcEpZ7dfwb9wH13a2oPMxdynwsJuonrLgrpJNrtIdWCEPLCHmhkltWvve1rJs2RqpC
p2AbsjJ5tnQJEsDkgH",
  "request_data": {
    "digest": "9D3407981112133A7FA74A804A300F93BD5520500AAD06008F1F8D898464132
B",
    "filename": "sample-data (1).csv",
    "url": "https://dlptest.com/sample-data.csv"
  },
  "request_token": "0E74F887F4B7D24C77CB9A197036E4ADC47FCE2EE3B86BB223FC6FCCA
5AE909B55C056FA95A576E52C3D9587AD7A7C34EDD2B14897EDD59D3265EB17310F56BDE
835DC02A991A8F372953517A038CAB4B5F2667F3479919850867E3FC2510719EE4604D5DD
F24D6A606C5821FA5F62F0B9D9F776A15B16C7871579BAEB09F656",
  "tab_url": "https://dlptest.com/sample-data.csv",
  "tags": [ "dlp", "malware" ]
}
```

```
[5/1/2021, 3:55:23 AM]
{
  "results": [ {
    "status": "SUCCESS",
    "tag": "dlp",
    "triggered_rules": [ {
      "action": "WARN",
      "rule_id": "245165307",
      "rule_name": "[jzhen] Test DLP rule"
    } ]
  }, {
    "status": "SUCCESS",
    "tag": "malware",
    "triggered_rules": [  ]
  } ],
  "token": "0E74F887F4B7D24C77CB9A197036E4ADC47FCE2EE3B86BB223FC6FCCA5AE909B
55C056FA95A576E52C3D9587AD7A7C34EDD2B14897EDD59D3265EB17310F56BDE835DC02
A991A8F372953517A038CAB4B5F2667F3479919850867E3FC2510719EE4604D5DDF24D6A6
06C5821FA5F62F0B9D9F776A15B16C7871579BAEB09F656"
}
```

chrome enterprise

Résolution des problèmes liés aux fonctionnalités de protection des données

Résolution des problèmes côté navigateur

chrome://safe-browsing/#tab-reporting

- Cet onglet affiche tous les journaux d'événements envoyés par Chrome au centre de sécurité. Vous trouverez ci-dessous un exemple de message de journal qui a été envoyé pour le déclencheur de protection contre la perte de données.


```
{
  "sensitiveDataEvent": {
    "clickedThrough": false,
    "contentSize": 4750,
    "contentType": "text/csv",
    "downloadDigestSha256": "9D3407981112133A7FA74A804A300F93BD5520500AAD06008F1F8D898464132B",
    "eventResult": "EVENT_RESULT_WARNED",
    "fileName": "/usr/local/google/home/jzhen/Downloads/sample-data (1).csv",
    "profileUserName": "jzhen@beyondcorp.joonix.net",
    "trigger": "FILE_DOWNLOAD",
    "triggeredRuleInfo": [ {
      "ruleId": "245165307",
      "ruleName": "[jzhen] Test DLP rule"
    } ],
    "url": "https://dlptest.com/sample-data.csv"
  },
  "time": "2021-05-01T03:55:23.143Z",
  "uploaded_successfully": true
}
```


- Si vous vous attendez à un certain comportement et que vous ne le voyez pas, utilisez l'une de ces URL dans un nouvel onglet pour voir si les journaux reflètent ce à quoi vous vous attendez.
- Remarque : Ces onglets doivent être OUVERTS au moment de la requête pour que les événements apparaissent.

Pour vérifier que les règles Chrome sont configurées, ouvrez un nouvel onglet Chrome dans la fenêtre du profil protégé, accédez à chrome://policy et cliquez sur "Actualiser les règles" pour vous assurer que la règle Chrome est mise à jour.

- En fonction de votre configuration, l'ensemble ou une partie des règles suivantes devraient être appliqués.

OnBulkDataEntryEnterpr…	{ "block_until_verdict": 0, "enable": [{ "tags": ["dlp"], "ur…	Cloud
OnFileAttachedEnterpris…	{ "block_large_files": false, "block_password_protected": false,…	Cloud
OnFileDownloadedEnter…	{ "block_large_files": false, "block_password_protected": false,…	Cloud
OnSecurityEventEnterpri…	{ "service_provider": "google" }	Cloud

chrome enterprise

Résolution des problèmes liés aux fonctionnalités de protection des données

Résolution des problèmes côté console

Cette section fournit quelques conseils pour résoudre les problèmes liés aux fonctionnalités de protection des données et de prévention des menaces dans la console d'administration Google à l'adresse admin.google.com.

- Assurez-vous que le compte utilisateur ou l'appareil géré pour lequel vous tentez de résoudre un problème dispose d'une licence Chrome Enterprise Premium.
  - Pour ce faire, accédez à Facturation > Abonnements, sélectionnez "Chrome Enterprise Premium" et cliquez sur le lien hypertexte bleu indiquant "Attribué" dans la colonne "Licences", puis recherchez l'appareil ou le compte utilisateur pour lequel vous tentez de résoudre un problème.
- Vérifiez que les paramètres Chrome Enterprise Premium sont appliqués pour "l'unité organisationnelle" dans laquelle se trouve l'appareil ou le compte d'utilisateur.
  - Pour ce faire, accédez aux "Paramètres" du navigateur Chrome, filtrez sur "Catégorie contient" "connecteur" et vérifiez que le paramètre suivant est correctement défini :
    - "Autoriser les connecteurs Enterprise" est défini sur "Autoriser les utilisateurs à activer les connecteurs Enterprise".
  - En fonction de la configuration de l'appareil, vous devrez peut-être vérifier que les éléments suivants sont définis sur "Chrome Enterprise Premium" dans le menu déroulant :
    - Importer l'analyse du contenu
    - Télécharger l'analyse du contenu
    - Analyse groupée du contenu textuel
    - Analyse du contenu imprimé
    - Vérification des URL en temps réel
  - Il est également conseillé de vérifier le paramètre "mode" sous "Paramètres supplémentaires" pour chaque fonctionnalité activée, car certaines peuvent être réglées sur "Désactivée par défaut, sauf pour les formats d'URL suivants".
- Si vous tentez de résoudre un problème lié à une règle spécifique (comme une règle de protection contre la perte de données recherchant des données sensibles), vérifiez qu'elle est appliquée à "l'unité organisationnelle" qui contient l'appareil ou le compte utilisateur en question.
  - Pour ce faire, dans la section "Règles", sélectionnez la règle pour laquelle vous tentez de résoudre un problème et contrôlez les points suivants :
    - Vérifiez que la règle est active.
    - Vérifiez que le champ d'application contient bien "l'unité organisationnelle" pour laquelle vous tentez de résoudre un problème.
    - Cliquez sur "Examiner une règle" pour voir si l'appareil ou le compte utilisateur en question apparaît dans les journaux comme ayant déclenché la règle.
  - Si les points ci-dessus sont corrects, cliquez sur "annuler" pour quitter l'éditeur de règles.
- Consultez ce guide pour résoudre les erreurs d'accès dans la console Google Cloud.

chrome enterprise

Questions fréquentes

Qu'est-ce que Chrome Enterprise Premium et combien cette solution coûte-t-elle ?

Chrome Enterprise Premium réunit le navigateur d'entreprise le plus fiable et les fonctionnalités de sécurité avancées de Google. Il s'appuie sur les fonctionnalités disponibles dans Chrome Enterprise Core et offre des fonctionnalités de sécurité avancées supplémentaires, y compris des commandes professionnelles, des insights sur la sécurité, des contrôles d'accès contextuels, ainsi que la protection des données et la prévention des menaces.

Les licences Chrome Enterprise Premium sont accordées sur la base d'une licence par compte utilisateur. Pour plus d'informations sur les tarifs, veuillez contacter votre conseiller commercial. Pour en savoir plus sur Chrome Enterprise Premium, cliquez ici.

chrome enterprise

Questions fréquentes

Chrome Enterprise Premium nécessite-t-il l'utilisation de Google Workspace ?

Non, Google Workspace n'est pas nécessaire. Chrome Enterprise Premium complète Google Workspace en ajoutant des protections de données supplémentaires à des solutions telles que Drive et Gmail, mais il n'est pas obligatoire de disposer de Google Workspace.

Quels sont les systèmes d'exploitation compatibles ?

Chrome Enterprise Premium est actuellement compatible avec toutes les plates-formes de bureau, y compris Windows, Mac, Linux et ChromeOS. iOS et Android sont tous deux compatibles pour l'accès mobile aux applications Web moyennant la mise en œuvre de règles d'accès contextuel.

Chrome Enterprise Premium est-il compatible avec tout type d'installation de Chrome ?

Les installations basées sur l'utilisateur et les installations gérées du navigateur Chrome sont toutes deux admises. Aucune version spéciale du navigateur Chrome n'est requise et aucun agent supplémentaire n'est nécessaire. La solution est donc facile à gérer et à déployer à l'aide de vos méthodes de gestion actuelles.

Qu'est-ce que Chrome Enterprise Core ?

Chrome Enterprise Core offre des fonctionnalités de gestion de base sans coût supplémentaire. Il permet aux équipes informatiques de centraliser la gestion et la sécurisation de Chrome au sein de leur organisation, quelle que soit la plate-forme des appareils. Pour en savoir plus, cliquez ici.

chrome enterprise

Questions fréquentes

Ai-je besoin de Google Workspace pour les protections basées sur l'utilisateur ?

Pas forcément. Vous pouvez utiliser Google Cloud Identity Free pour gérer les comptes utilisateur et/ou synchroniser votre fournisseur d'identité actuel avec Google pour fournir des protections basées sur l'utilisateur.

Chrome Enterprise Premium est-il compatible avec d'autres navigateurs ?

Actuellement, Chrome Enterprise Premium ne fonctionne qu'avec Google Chrome, mais certaines fonctionnalités de la solution peuvent empêcher que d'autres navigateurs n'accèdent à vos données sensibles.

Chrome Enterprise Premium est-il compatible avec les fenêtres de navigation privée ?

La solution n'est pas compatible avec les activités effectuées dans les fenêtres de navigation privée. Pour savoir comment empêcher les utilisateurs d'ouvrir de nouvelles fenêtres de navigation privée, consultez l'article concernant le paramètre Mode navigation privée.

Quelles sont les données collectées par Chrome Enterprise Premium ?

Les données collectées varient en fonction de la configuration définie par l'administrateur.

- Si l'appareil est enregistré dans la gestion cloud du navigateur Chrome avec la fonction de création de rapports activée, alors vous pouvez vous référer à ce document pour en savoir plus sur les données collectées.
- Si la création de rapports sur les événements liés à la sécurité Chrome est activée, alors vous pouvez vous référer à ce document pour en savoir plus sur les données collectées.
- Des informations supplémentaires sur les événements et les attributs de journaux Chrome sont disponibles via ce lien.

chrome enterprise

Autres ressources

Chrome Enterprise Premium

- Vue d'ensemble de Chrome Enterprise Premium

Gestion du navigateur

- Présentation de la gestion cloud du navigateur Chrome
- Configurer la gestion cloud du navigateur Chrome
- Guide de gestion cloud du navigateur Chrome

Intégrations tierces

- Connecteurs de création de rapports pour le navigateur Chrome
- Connecteurs de confiance des appareils pour le navigateur Chrome
- Connecteurs de protection contre la perte de données pour le navigateur Chrome