chrome enterprise

Premiers pas : Un guide pour gérer les extensions du navigateur Chrome en entreprise

Introduction

Des milliers d'extensions sont disponibles pour le navigateur Chrome, dont un grand nombre particulièrement utiles pour faire gagner du temps aux utilisateurs, améliorer les workflows de leur entreprise et optimiser leur efficacité. Qu'elles vous permettent d'optimiser la RAM, d'augmenter les vitesses de navigation ou de corriger votre grammaire, les extensions sont conçues pour doper votre productivité au bureau. Sans une gestion appropriée, toutefois, elles peuvent également présenter un risque et introduire des failles dans votre environnement professionnel. Les équipes informatiques doivent donc trouver un juste équilibre entre les besoins de productivité des utilisateurs et la sécurité de l'entreprise.

En matière de gestion des extensions, les priorités des équipes informatiques en entreprise sont de trois ordres :

1. Protéger les données des utilisateurs et de l'entreprise
2. Prévenir l'installation d'extensions malveillantes
3. Garantir aux utilisateurs l'accès aux extensions dont ils ont besoin pour gagner en productivité et en efficacité

Avec autant d'extensions inédites et existantes, et de mises à jour constantes, il est vital que les administrateurs suivent les bonnes pratiques pour surveiller, gérer et sécuriser les extensions Chrome de leurs utilisateurs.

Ce document technique va vous présenter les différentes options de gestion à votre disposition et vous aider à choisir la méthode la mieux adaptée à vos besoins.

Critères à prendre en compte

Avant de gérer des extensions, commencez par identifier les critères sur lesquels votre organisation se basera pour évaluer et approuver ces extensions. Pour ce faire, vous pouvez répondre aux questions suivantes :

- Quelles sont les réglementations en matière de sécurité et les mesures de conformité que votre organisation doit respecter ?
- Quelles données de l'utilisateur et de l'entreprise sont actuellement stockées sur les appareils de vos utilisateurs ?
- Quelles autorisations requises par les extensions seraient susceptibles d'enfreindre vos règles en matière de sécurité des données ?

Une fois que vous avez les réponses à ces questions, vous êtes prêt à étudier les options de gestion des extensions à votre disposition.

L'approche traditionnelle

Pendant longtemps, la seule manière de gérer les extensions de navigateur était de les évaluer une par une manuellement avant de créer des listes d'autorisation et de blocage afin de déterminer les extensions à installer ou non sur les appareils des utilisateurs. Certaines organisations recourent encore à cette approche.

La console d'administration Google vous permet :

- d'autoriser toutes les extensions, à l'exception de celles que vous voulez bloquer ;
- de bloquer toutes les extensions, à l'exception de celles que vous voulez autoriser ;
- de bloquer ou d'autoriser des extensions spécifiques ;
- d'installer d'office une ou plusieurs extensions.

Dans la stratégie de groupe Microsoft[1], les modèles vous permettent d'appliquer à certains groupes ou à toute l'organisation des mesures de protection semblables, y compris :

- Autoriser toutes les extensions, à l'exception de celles que vous voulez bloquer
- Bloquer ou autoriser une extension
- Installer d'office une extension

Ces deux approches fonctionnent jusqu'à un certain point. Elles présentent des limites et requièrent beaucoup d'énergie de la part des utilisateurs, car leur gestion est essentiellement manuelle.

Le temps nécessaire à l'examen des extensions peut nuire à la productivité des administrateurs et des utilisateurs. Plus important encore en termes de sécurité, les extensions déjà ajoutées à votre liste blanche peuvent être rachetées et/ou mises à jour par des entités que vous n'avez pas approuvées.

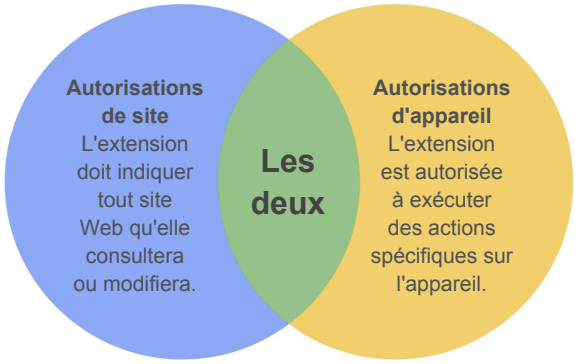
[1] Microsoft®, Windows® et Internet Explorer® sont des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays.

Une approche moderne : gérer les extensions en fonction des autorisations

Pour vous aider à gérer les extensions de manière plus efficace, évolutive et sécurisée dans votre entreprise, Chrome vous permet également de les gérer en fonction des autorisations. Grâce à cette méthode, les équipes informatiques peuvent mettre les extensions nécessaires à disposition des utilisateurs sans exposer les données de l'entreprise. Il s'agit de la méthode que l'équipe informatique Google utilise et recommande aux autres entreprises.

Les autorisations permettent à une extension d'apporter des modifications à un site Web ou à un appareil. Pour qu'une extension s'exécute correctement, des autorisations précises sont souvent requises.

Il en existe deux catégories principales : les autorisations de site et les autorisations d'appareil. Un grand nombre d'extensions utilisent les deux.



Exemples d'autorisations associées aux sites : autoriser une extension à bloquer des images ou à contrôler le degré de zoom sur un site. Exemples d'autorisations associées aux appareils : accéder à des ports USB, afficher l'écran et interagir avec des programmes.

Pour limiter encore plus les risques, envisagez de gérer les extensions à l'aide des règles suivantes :

- **Autorisations bloquées/acceptées :** permet d'empêcher que des extensions déjà en liste blanche soient mises à jour avec de nouvelles autorisations. Vous pouvez par ailleurs désactiver les extensions déjà installées qui ne répondraient plus à vos besoins.
- **Hôtes bloqués pendant l'exécution :** permet de spécifier les sites sur lesquels les extensions peuvent s'exécuter.
- **Extensions installées d'office :** permet d'installer d'office des extensions sur les machines de vos utilisateurs pour qu'ils disposent des outils de productivité dont ils ont besoin.
- **Listes d'autorisation/de blocage :** si nécessaire.

Cette méthode de gestion des extensions Chrome, plus sécurisée et plus simple, est parfaitement adaptée aux organisations de grande taille. Elle protège les utilisateurs des extensions malveillantes et fait gagner du temps à l'équipe informatique qui n'a plus besoin de gérer de longues listes d'autorisation ou de blocage, de passer en revue les mises à jour ou d'approuver les extensions une par une. Cette méthode ne présente que des avantages.

chrome enterprise

Premiers pas : gérer des extensions en fonction des autorisations

Pour commencer à gérer les extensions de votre entreprise en fonction des autorisations, procédez comme suit :

1. Dressez la liste des extensions déjà installées par vos utilisateurs (utilisez les rapports de la gestion cloud du navigateur Chrome ou interrogez vos utilisateurs).

2. Identifiez les sites Web/hôtes qui doivent être sécurisés. Déterminez les autorisations susceptibles d'être risquées et devant être restreintes.

3. Créez une liste de toutes les données collectées et partagez-la avec les principales parties prenantes pour obtenir leur adhésion.

4. Testez vos nouvelles règles dans un environnement test ou au sein d'un groupe pilote restreint, puis déployez-les en plusieurs phases dans l'entreprise.

5. Lisez les commentaires laissés par les utilisateurs.

6. Répétez cette procédure et ajustez-la tous les mois, tous les trimestres ou tous les ans (en fonction des besoins de votre organisation).

Pour mettre en œuvre un ensemble d'autorisations acceptées et protéger les sites sensibles de votre entreprise, vous n'avez à définir ces règles qu'une seule fois. Votre entreprise gagnera automatiquement en sécurité, et l'expérience de vos utilisateurs en sera améliorée.

Vos collaborateurs pourront même être en mesure d'installer des extensions qu'il leur était impossible d'installer avant, mais ils ne seront pas autorisés à les exécuter sur les sites sensibles de l'entreprise.

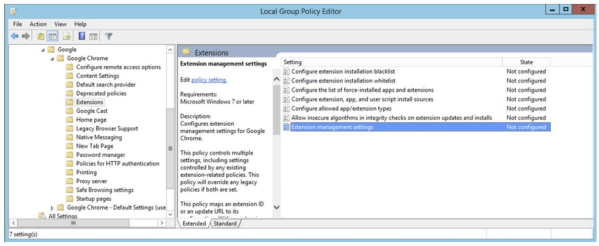
[2] Mac et macOS sont des marques d'Apple Inc., déposées aux États-Unis et dans d'autres pays.

Configurer des autorisations

Vous pouvez facilement définir les extensions que vos utilisateurs sont autorisés à installer. Il vous suffit pour cela d'indiquer les autorisations acceptables et celles qui ne le sont pas.

Console d'administration Google

Dans les environnements Windows, Chrome OS, Mac[2] et Linux, vous pouvez utiliser la console d'administration Google pour configurer ces paramètres. Si une extension exige un accès ou des autorisations contraires à vos règles de sécurité, elle ne sera pas installée. Par exemple, vous pouvez bloquer une extension qui se connecte aux appareils USB de vos utilisateurs ou empêche l'accès aux cookies. Si une extension installée requiert une autorisation bloquée, elle ne s'exécutera pas. Dans ce cas,
elle n'est pas supprimée, mais désactivée.



Stratégie de groupe

Vous avez également la possibilité de gérer les extensions sous Windows en utilisant les règles des paramètres d'extension. Avec l'éditeur de gestion des stratégies de groupe, vous pouvez définir plusieurs règles de manière centralisée à l'aide d'une chaîne JSON ou du Registre Windows. Cette méthode courante vous permet de contrôler un certain nombre de paramètres, comme le mode d'installation,

l'URL de mise à jour, les autorisations bloquées, les sources d'installation, les types autorisés, les installations bloquées, ainsi que les hôtes bloqués et autorisés pendant l'exécution. Vous pouvez choisir de définir l'ensemble des paramètres de gestion des extensions à cet emplacement, ou de les configurer par le biais d'autres règles. La configuration s'effectue dans le Registre Windows ou via une chaîne JSON dans l'éditeur de stratégies de groupe Windows.

Autres considérations

Certaines organisations préfèrent déployer leur propre site pour télécharger les extensions. Google ne recommande pas cette approche, moins sûre que le Chrome Web Store. Celui-ci permet en effet d'analyser les codes automatiquement et manuellement afin de prévenir l'envoi de codes malveillants aux utilisateurs.

La gestion cloud du navigateur Chrome est une nouvelle console qui vous permet de gérer, de manière centralisée, les paramètres de votre navigateur Chrome sur vos machines Windows, Mac et Linux. Elle offre une vue détaillée de l'état du navigateur Chrome dans votre environnement, en vous fournissant instantanément des informations sur :

- les versions du navigateur Chrome actuellement déployées dans votre parc d'ordinateurs de bureau et portables, quel que soit leur type ;
- les extensions installées dans chaque navigateur ;
- les règles appliquées à chaque navigateur.

La console vous permet également de bloquer en un clic toute extension suspecte sur l'ensemble de vos ordinateurs.

Gérer les extensions Chrome de la même manière que Google

Après avoir utilisé pendant des années la méthode de gestion des extensions traditionnelle sur plus de 300 000 points de terminaison, l'équipe informatique interne de Google a compris qu'il fallait créer une approche moins laborieuse, capable d'établir un juste milieu entre les besoins informatiques de l'entreprise et la sécurité, tout en optimisant la productivité de ses collaborateurs. La méthode consistant à gérer les extensions en fonction des autorisations est une solution évolutive et sécurisée qui réduit considérablement sa charge de travail.

À l'image de Google, vous pouvez vous aussi opter pour la méthode plus sécurisée décrite dans ce document. Vous offrirez ainsi à votre entreprise la sécurité dont elle a besoin, tout en permettant à vos utilisateurs d'installer des extensions sûres, qui doperont leur productivité.

Passez dès aujourd'hui à la gestion des extensions basée sur les autorisations.

Pour plus d'informations sur la gestion des extensions du navigateur Chrome, **consultez les ressources suivantes :**

Lisez le guide de gestion des extensions en entreprise.
Regardez la session en petit groupe Google Cloud Next '19 : comment l'équipe informatique Google Cloud gère les extensions en entreprise.
Passez en revue les options de gestion cloud du navigateur Chrome.
Consultez les téléchargements du navigateur Chrome dans votre entreprise.
Renseignez-vous sur l'assistance Enterprise pour le navigateur Chrome.
Consultez la liste des règles du navigateur Chrome.
Visitez le Centre d'aide du navigateur Chrome pour les entreprises et le forum d'aide sur le navigateur Chrome.