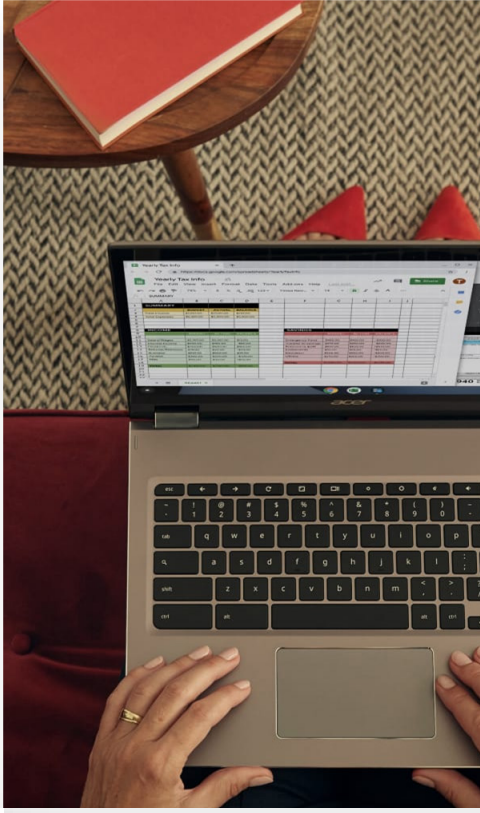
chrome

Guide de configuration de la sécurité du navigateur Chrome pour les entreprises

Basé sur Chrome 90

chrome

Guide de configuration de la sécurité du navigateur Chrome pour les entreprises



Basé sur Chrome 90

Dernière mise à jour : 20 mai 2021

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

Objet de ce guide

Ce document traite du navigateur Chrome sur le système d'exploitation Windows, mais la plupart des conseils qu'il rassemble s'appliquent également aux autres plates-formes pour ordinateurs. Les administrateurs auront des compromis à faire entre la sécurité de leur organisation et les technologies et fonctionnalités auxquelles leurs utilisateurs souhaitent avoir accès.

Ce document décrit dans le détail les différentes règles de sécurité disponibles pour Chrome, et ce que leur activation/désactivation implique.

Sujets abordés

Ce document regroupe des recommandations et des considérations essentielles pour les organisations vigilantes qui souhaitent activer ou désactiver des règles de sécurité de Chrome.

Audience principale

Administrateurs de Microsoft® Windows® et du navigateur Chrome

Environnement informatique

Microsoft Windows 7 et versions ultérieures

Enseignements

Éléments déterminant le choix entre sécurité de l'entreprise et impact sur les utilisateurs lorsqu'on définit des règles de sécurité pour le navigateur Chrome.

Introduction

Le navigateur Chrome est fait pour assurer la sécurité des internautes. L'équipe Chrome prend cette question au sérieux, et nous sommes fiers de notre réputation de leader dans ce domaine avec différentes innovations telles que les bacs à sable, les normes TLS et la sécurité sans compromis sur la facilité d'utilisation.

La configuration par défaut du navigateur Chrome vise l'équilibre entre sécurité et facilité d'utilisation de manière à offrir une expérience optimale à tous les internautes. Cependant, les entreprises peuvent avoir des objectifs quelque peu différents lorsqu'elles utilisent un navigateur sécurisé dans leur organisation, et ce document décrit les options dont elles disposent pour configurer Chrome en fonction de ces objectifs.

Par défaut, Chrome se comporte de manière à concilier facilité d'utilisation et sécurité. Or, il arrive parfois que ces deux paramètres entrent en conflit. Dans de tels cas, Chrome met à votre disposition une règle qui vous permet de faire un choix. En tant qu'administrateur informatique, il vous appartient de déterminer quelle est la règle la mieux adaptée à ces cas précis.

Ce document décrit diverses situations impliquant un choix entre facilité d'utilisation et sécurité, ainsi que les avantages et inconvénients associés à chaque option. Dans chaque cas, vous devez peser le pour et le contre afin de trouver le paramètre qui convient le mieux à l'environnement de votre entreprise.

Nous examinerons trois aspects différents de la sécurité des entreprises :

- Prévention des menaces
- Confidentialité
- Gestion et performances

Les recommandations présentées ici font généralement référence à des paramètres particuliers de règles documentés de façon exhaustive sur la page https://chromeenterprise.google/policies.

Prévention des menaces

Chrome offre déjà des protections contre les menaces liées aux sites Web malveillants :

- L'isolation de sites isole chaque site dans un espace mémoire (processus du système d'exploitation) qui lui est propre. Pour en savoir plus sur cette option, consultez cet article du Centre d'aide.
- Ces processus s'exécutent eux-mêmes dans des bacs à sable pour limiter le risque qu'une autre partie de l'ordinateur soit victime d'une faille.
- La navigation sécurisée analyse le Web et classifie les dangers en permanence de manière à détecter les contenus et les logiciels malveillants ou trompeurs. Cette fonctionnalité avertit les utilisateurs avant qu'ils accèdent à un site signalé comme potentiellement dangereux.

Ainsi, Chrome est un navigateur sécurisé à la conception avec des paramètres par défaut qui favorisent la sécurité des internautes sur le Web, mais deux méthodes de configuration s'offrent à vous pour renforcer la prévention des menaces :

- Imposer la configuration par défaut de Chrome aux utilisateurs de sorte qu'ils ne puissent pas la modifier
- Renforcer la sécurité en faisant des compromis entre facilité d'utilisation et sécurité

Les deux sous-sections qui suivent présentent plusieurs configurations possibles selon ces deux méthodes.

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

chrome

Dernière mise à jour : 20 mai 2021

Paramètres imposant le comportement par défaut actuel de Chrome

Chrome est sécurisé à la base. Cela signifie que ses paramètres par défaut privilégient la sécurité des utilisateurs pour leur offrir l'expérience la plus sûre possible. Les utilisateurs peuvent modifier certains paramètres s'ils souhaitent changer le comportement de leur navigateur, mais cela peut avoir une incidence sur la sécurité. C'est pourquoi les administrateurs ont la possibilité d'imposer certains paramètres à l'aide de règles.

Besoin de l'entreprise	Impact sur l'utilisateur	Impact potentiel sur la sécurité	Options et remarques

Je souhaite m'assurer qu'aucune règle dangereuse pour mon organisation n'a été définie par un ancien administrateur.	● Aucun	● Aucun	Vérifiez que les règles suivantes n'ont pas été définies pour être sûr de bénéficier de la configuration par défaut (la plus sûre) :
			
			`EnableDeprecatedWebPlatformFeatures`
			`RunAllFlashInAllowMode`
			`SuppressUnsupportedOSWarning`
			`EnableOnlineRevocationChecks`
			`OverrideSecurityRestrictionsOnInsecureOrigin`
			`CertificateTransparencyEnforcementDisabledForCas`
			`CertificateTransparencyEnforcementDisabledForLegacyCas`
			`LegacySameSiteCookieBehaviorEnabled`
			`LegacySameSiteCookieBehaviorEnabledForDomainList`
			`ChromeVariations`
			`DnsOverHttpsMode`
			`LookalikeWarningAllowlistDomains`
			`SafeBrowsingAllowlistDomains`
			`RemoteAccessHostAllowRemoteAccessConnections`
			
			Cette liste n'est pas exhaustive, mais comprend les principales règles de sécurité utilisées par les entreprises. Pour connaître les autres options associées aux règles, consultez notre liste des règles Chrome Enterprise.

Je souhaite faire en sorte que les utilisateurs ne puissent pas désactiver les fonctionnalités de sécurité essentielles.	● Aucun	● Aucun	Définissez explicitement les règles `AllowOutdatedPlugins`, `SafeBrowsingProtectionLevel` et `ThirdPartyBlockingEnabled`. Les utilisateurs bénéficieront de la même expérience, si ce n'est qu'ils ne pourront pas modifier ces paramètres.

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

Paramètres imposant le comportement par défaut actuel de Chrome (suite)

Besoin de l'entreprise	Impact sur l'utilisateur	Impact potentiel sur la sécurité	Options et remarques
Je souhaite empêcher les utilisateurs de télécharger des logiciels malveillants, les protéger de l'hameçonnage, et faire en sorte qu'ils ne puissent pas désactiver ces protections.	Faible	Aucun	La navigation sécurisée est une fonctionnalité de Chrome qui vise à protéger les utilisateurs des téléchargements de logiciels malveillants et de l'hameçonnage. Pour en savoir plus, consultez Utiliser la navigation sécurisée dans Chrome. Certaines entreprises sont tentées de désactiver la navigation sécurisée, car elles estiment que leurs produits de sécurité existants (antivirus, pare-feu) remplissent les mêmes fonctions. La navigation sécurisée et votre solution peuvent agir de façon complémentaire. Par exemple, les antivirus traitent avant tout le contenu des téléchargements, alors que la navigation sécurisée cible davantage leur contexte, à savoir la chaîne de navigation qui a amené l'utilisateur au lien en question. Si vous désactivez la navigation sécurisée, vous perdez le bénéfice de ces informations. L'équipe Chrome chargée de la sécurité vous recommande de maintenir la navigation sécurisée activée. Pour empêcher les utilisateurs de désactiver cette fonctionnalité, définissez la règle `SafeBrowsingProtectionLevel` sur "1" afin que la navigation sécurisée soit active en mode standard. Rien ne changera pour les utilisateurs, si ce n'est qu'ils ne pourront plus désactiver la navigation sécurisée. Dans M79, nous avons annoncé la navigation sécurisée avec protection renforcée pour Chrome, une nouvelle option offrant un niveau de sécurité plus avancé aux utilisateurs qui en ont besoin ou qui souhaitent en bénéficier lorsqu'ils naviguent sur le Web. Une fois activée, cette fonctionnalité renforce significativement la protection contre les sites Web et les téléchargements malveillants. La navigation sécurisée Google transmet des données en temps réel à Chrome afin qu'il protège les utilisateurs de façon proactive contre les sites dangereux. Vous pouvez activer la navigation sécurisée avec protection renforcée en définissant la règle `SafeBrowsingProtectionLevel` sur "2".

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

Paramètres imposant le comportement par défaut actuel de Chrome (suite)

Besoin de l'entreprise	Impact sur l'utilisateur	Impact potentiel sur la sécurité	Options et remarques
Je souhaite empêcher les utilisateurs de télécharger des logiciels malveillants, les protéger de l'hameçonnage, et faire en sorte qu'ils ne puissent pas désactiver ces protections.	Faible	Aucun	Vous pouvez appliquer la navigation sécurisée de façon plus agressive en définissant la règle : `DisableSafeBrowsingProceedAnyway` Cela peut avoir un impact sur l'utilisateur, qui ne pourra pas poursuivre sa navigation sur le site Web même lorsque la navigation sécurisée estime à tort qu'il s'agit d'un site d'hameçonnage. Vous pouvez aussi définir la règle `DownloadRestrictions` sur "2" afin d'appliquer les décisions de la navigation sécurisée de manière un peu plus stricte. Pour en savoir plus, consultez Empêcher les utilisateurs de télécharger des fichiers dangereux. Certaines entreprises choisissent de bloquer aussi les impressions, considérant que les impressions dans des fichiers PDF constituent un moyen d'accès au disque pour les logiciels malveillants. L'équipe Chrome chargée de la sécurité ne pense pas qu'une telle mesure soit utile. Dans la grande majorité des cas, la conversion d'une page Web en fichier PDF élimine tout contenu malveillant, mais nous vous recommandons d'utiliser une visionneuse PDF sécurisée pour les fichiers enregistrés de cette manière (Chrome par exemple).
J'envisage d'utiliser un logiciel tiers qui requiert l'injection de code dans Chrome.	Élevé	Élevé	Chrome empêche les logiciels tiers installés sur l'ordinateur d'injecter leur propre code dans Chrome. Les injections de code tiers se sont avérées être une source majeure de plantages et de bugs qui peuvent (en théorie) être exploités par des sites Web malveillants. C'est pourquoi nous recommandons de conserver le paramètre par défaut (`ThirdPartyBlockingEnabled` sur "True"). D'autres produits de sécurité peuvent vous demander de débloquer leur code pour les autoriser à se servir de Chrome ou à modifier son comportement. Si vous choisissez de le faire, vous pourrez bénéficier de leur fonctionnalité, mais le nombre de plantages et le risque de failles exploitables seront plus élevés. Si vous utilisez un produit de sécurité qui injecte du code exécutable dans Chrome, demandez au fournisseur s'il propose une extension Chrome offrant la même fonctionnalité.

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

Paramètres qui limitent la fonctionnalité utilisateur, mais réduisent la surface d'attaque

Vous pouvez altérer la fonctionnalité de Chrome pour réduire la surface d'attaque des sites Web malveillants. Chaque élément bloqué représente une dégradation de la fonctionnalité pour l'utilisateur.

Pour la plupart, ces changements consistent à désactiver des fonctionnalités Chrome. Nous tenons à souligner que les fonctionnalités Chrome sont toutes conçues et configurées à la base pour la sécurité. Par conséquent, vous ne devriez pas avoir à les désactiver. Cependant, nous savons que de nombreuses entreprises souhaitent ou doivent apporter de telles modifications. Vous trouverez ci-dessous divers éléments à prendre en compte pour orienter ces décisions.

Besoin de l'entreprise	Impact sur l'utilisateur	Impact potentiel sur la sécurité	Options et remarques
Mon organisation utilise ses propres certificats racines de confiance sur ses points de terminaison pour authentifier les serveurs de l'entreprise. Si des pirates informatiques volent la clé privée de ces certificats racines de confiance, je dois être en mesure de les révoquer.	Faible	Aucun	Vous pouvez activer des contrôles de révocation pour de tels certificats avec la règle `RequireOnlineRevocationChecksForLocalAnchors` Chrome ne garantit pas de pouvoir distinguer des certificats à partir d'ancrages locaux, car cela dépend des caractéristiques du système d'exploitation, qui varient d'une plate-forme et d'une version à l'autre. Si la révocation n'est pas accessible, ces certificats ne sont pas utilisables (échec forcé), ce qui peut empêcher l'accès à certains sites Web.
D'anciennes versions de Chrome exécutées dans mon environnement peuvent être exploitées par des sites Web malveillants.	Faible	Aucun	Vous pouvez forcer les utilisateurs à relancer Chrome pour obtenir les mises à jour plus rapidement à l'aide des règles `RelaunchNotification` et `RelaunchNotificationPeriod`. Nous recommandons vivement cette configuration aux entreprises, car elle permet de s'assurer que les utilisateurs disposent de la version de Chrome la plus récente et des derniers correctifs de sécurité.
Je souhaite éviter que les mots de passe des utilisateurs soient interceptés lors de transferts Internet utilisant des protocoles d'authentification anciens (authentification digest, de base).	Faible	Aucun	Vous pouvez désactiver ces anciens schémas avec la règle `AuthSchemes`. Peu de sites Web légitimes récents utilisent ces schémas. Il est donc judicieux de les désactiver dans le contexte d'une entreprise. Depuis Chrome 75, nous recommandons NTLM et Negotiate. Assurez-vous que les services de votre entreprise utilisent eux aussi des mécanismes d'authentification modernes.

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

Paramètres qui limitent la fonctionnalité utilisateur, mais réduisent la surface d'attaque (suite)

Besoin de l'entreprise	Impact sur l'utilisateur	Impact potentiel sur la sécurité	Options et remarques
Je souhaite empêcher l'envoi de documents provenant du cloud à des imprimantes vulnérables.	Faible	Aucun	Pour bloquer la réception de documents Google Cloud Print sur les imprimantes de votre entreprise, configurez la règle `CloudPrintProxyEnabled`.
Je crains que des pirates informatiques déjà introduits dans le réseau altèrent WPAD pour opérer un déplacement latéral.	Faible	Aucun	Vous pouvez utiliser la règle `ProxyMode` pour désactiver la découverte automatique du proxy.
Je crains que le téléchargement automatique de fichiers offre aux pirates informatiques la possibilité de nous attaquer par implantation de DLL ou de transférer des hachages de mots de passe vers des serveurs SMB malveillants. Je souhaite désactiver le téléchargement automatique.	Moyen	Aucun	Pour avertir l'utilisateur à chaque téléchargement, modifiez la règle `PromptForDownloadLocation`.
Je souhaite désactiver les graphismes 3D, car je pense qu'ils augmentent la surface d'attaque et que peu des sites Web consultés par nos utilisateurs les requièrent.	Moyen	Aucun	Vous pouvez les désactiver avec la règle `Disable3DAPIs`. Chrome offre déjà des protections significatives contre les attaques liées aux graphismes 3D, y compris un niveau appelé "ANGLE" dont le rôle est de nettoyer les entrées 3D et l'isolation de tout le code associé au processeur graphique dans un processus en bac à sable. La désactivation de WebGL empêchera les produits de cartographie virtuelle de fonctionner.
Je souhaite réduire le risque qu'un site Web lance une attaque par canal auxiliaire pour extraire des données d'un autre site Web.	Moyen	Aucun	Vous pouvez affiner l'isolation de sites à l'aide de la règle `IsolateOrigins`. Pour en savoir plus, consultez Protéger ses données avec l'isolation de sites. Remarque : Cette configuration utilise davantage de mémoire.

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

Paramètres qui limitent la fonctionnalité utilisateur, mais réduisent la surface d'attaque (suite)

Besoin de l'entreprise	Impact sur l'utilisateur	Impact potentiel sur la sécurité	Options et remarques
Je souhaite empêcher des utilisateurs externes de prendre le contrôle des ordinateurs de notre réseau via le Bureau à distance Chrome.	Moyen	Aucun	Vous pouvez bloquer l'application Bureau à distance Chrome de la même manière que toute autre application ou extension. Pour en savoir plus, consultez Contrôler l'utilisation du Bureau à distance Chrome.
Je souhaite désactiver les extensions et les applications, car je pense qu'elles augmentent la surface d'attaque, et l'impact sur les processus de travail des utilisateurs m'importe peu.	Élevé	Faible	Vous risquez de freiner significativement la productivité des utilisateurs si vous désactivez toutes les extensions. Par ailleurs, certaines extensions sont faites pour renforcer la sécurité des utilisateurs, par exemple les gestionnaires de mots de passe tiers utilisés à titre personnel. Nous vous recommandons de gérer les extensions par autorisation : 1. Bloquez l'installation des extensions nécessitant des autorisations que vous jugez dangereuses et autorisez toutes les autres. 2. Bloquez l'accès des extensions restantes aux hôtes sensibles. Par exemple, vous pouvez autoriser toutes les extensions à l'exception de celles qui utilisent la webcam ou enregistrent des captures d'écran, tout en empêchant toute autre extension d'accéder aux sites les plus précieux de votre entreprise. Pour plus d'informations, consultez Autorisations relatives aux applications et aux extensions Chrome et parcourez le livre blanc sur la gestion des extensions dans votre entreprise. Vous pouvez aussi demander à votre spécialiste Chrome Enterprise de vous fournir d'autres ressources expliquant pourquoi les entreprises choisissent cette approche. Si vous ne parvenez pas à identifier les autorisations qui vous posent problème, vous pouvez bloquer des extensions individuellement en définissant la règle `ExtensionInstallBlacklist`. Si vous saisissez la valeur "*" dans la liste de blocage, toutes les extensions sont ajoutées à la liste de blocage, sauf celles spécifiquement répertoriées dans la liste d'autorisation. Envisagez la mise en place d'un processus d'approbation des extensions ajoutées. Nous ne recommandons pas cette approche qui consiste à bloquer/autoriser les extensions individuellement, car elle n'est pas évolutive. Toutes les extensions Chrome doivent être distribuées directement par le Chrome Web Store ou par l'un des mécanismes décrits ci-dessous. Lisez la suite pour en savoir plus sur les extensions externes. La règle `BlockExternalExtensions` permet d'empêcher l'installation d'extensions externes.

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

Paramètres qui limitent la fonctionnalité utilisateur, mais réduisent la surface d'attaque (suite)

Besoin de l'entreprise	Impact sur l'utilisateur	Impact potentiel sur la sécurité	Options et remarques
#Je souhaite empêcher les utilisateurs d'ajouter des exceptions pour autoriser les contenus mixtes sur des sites spécifiques.	Élevé	Faible	DefaultInsecureContentSetting permet de contrôler l'utilisation d'exceptions pour le contenu non sécurisé. Si cette règle n'est pas configurée, les utilisateurs peuvent ajouter des exceptions qui autorisent l'affichage de contenu mixte blocable, et désactiver les mises à jour automatiques pour le contenu mixte blocable en option.
#Je souhaite corriger à distance les problèmes pouvant être causés par les cookies ou le cache sur les appareils des utilisateurs.	Élevé	Aucun	Vous pouvez envoyer des commandes à distance depuis la console d'administration pour effacer les cookies et le cache.

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

Confidentialité

Chrome est engagé dans la protection de la confidentialité des utilisateurs. De manière générale, les entreprises souhaitent limiter autant que possible les informations permettant d'identifier personnellement les utilisateurs et les données à caractère personnel (les "informations personnelles") stockées sur leurs ordinateurs, mais elles ne savent pas toujours à quel point Chrome protège ces données.

Certaines des fonctionnalités de sécurité les plus solides de Chrome (par exemple, la navigation sécurisée et le gestionnaire de mots de passe) impliquent des échanges d'informations avec les services Google. L'équipe Chrome chargée de la sécurité recommande vivement d'activer ces fonctionnalités. Si vous avez des doutes concernant l'utilisation des données ainsi envoyées, veuillez en parler à votre spécialiste Chrome Enterprise.

Les besoins des entreprises concernent trois catégories de données :

- Informations personnelles stockées sur les appareils de l'entreprise
- Données transmises sur Internet
- Données transmises à Google

Paramètres concernant les informations stockées sur les appareils de l'entreprise qui permettent d'identifier personnellement l'utilisateur

Besoin de l'entreprise	Impact sur l'utilisateur	Impact potentiel sur la sécurité	Options et remarques
Je crains que des utilisateurs (**non administrateurs**) qui se connectent à une même machine (successivement, ou simultanément via VDI) puissent accéder à des données sensibles d'autres utilisateurs, par exemple les mots de passe enregistrés sur le disque de la machine. Je crains que des voleurs puissent lire les mots de passe stockés sur le disque d'une machine après l'avoir dérobée.	N/A	N/A	Toutes les informations personnelles de l'utilisateur (historique de navigation, cache, mots de passe, données de saisie automatique) sont stockées dans un paquet d'informations appelé "profil". Les profils utilisateur sont protégés par les modèles d'autorisations standards du système d'exploitation et ne sont pas accessibles depuis les autres comptes utilisateur qui se connectent sur la machine. Lorsqu'un autre utilisateur ou un voleur obtient des droits d'accès illimités à la machine, il est évidemment en mesure de lire ces fichiers. Cependant, les éléments les plus sensibles du profil Chrome (par exemple, les mots de passe et les informations de carte de crédit) sont chiffrés à l'aide de l'API de protection des données (DPAPI) de Microsoft. Ce mode de fonctionnement est spécialement conçu pour rendre ces données inaccessibles aux administrateurs et autres personnes qui disposent d'un accès complet au disque et chiffre les données à l'aide du mot de passe de connexion de l'utilisateur. (Pour plus d'informations, consultez la documentation de la DPAPI Microsoft. Les administrateurs peuvent être en mesure de déchiffrer ces données s'ils ont accès aux clés privées stockées sur un contrôleur de domaine). Ainsi, les seuls cas dans lesquels des précautions spécifiques seraient requises sont les suivants : • Accès physique au disque par des administrateurs ou d'autres personnes • Accès aux données du profil Chrome (par exemple, cache du navigateur et autres éléments) qui ne sont pas chiffrées Passez à la ligne suivante du tableau si ces questions vous préoccupent.

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

Paramètres concernant les informations stockées sur les appareils de l'entreprise qui permettent d'identifier personnellement l'utilisateur (suite)

Besoin de l'entreprise	Impact sur l'utilisateur	Impact potentiel sur la sécurité	Options et remarques
Je crains que des **administrateurs** qui se connectent à une même machine (successivement, ou simultanément via VDI) puissent accéder à des données sensibles d'autres utilisateurs, par exemple le cache du navigateur stocké sur le disque de la machine.	● Élevé	● Aucun	Il s'agit d'un cas très spécifique, et la plupart des entreprises ne prennent pas de mesure spéciale pour s'en protéger. Notez que les données les plus sensibles comme les mots de passe et les numéros de carte de crédit ne sont pas concernées par ce type d'accès (plus d'informations à la ligne précédente du tableau). Si l'accès des administrateurs aux données moins sensibles des profils utilisateur (cache du navigateur, par exemple) vous préoccupe, utilisez la règle `ForceEphemeralProfiles` associée à l'obligation pour les utilisateurs de se connecter à Chrome (`ForceBrowserSignin`) de sorte que leurs favoris et autres préférences principales soient téléchargés à chaque fois. Si vous le souhaitez, vous pouvez aussi désactiver `BackgroundModeEnabled` afin de limiter la durée de chaque session. L'impact est important pour les utilisateurs, car ils doivent se connecter à Chrome chaque fois qu'ils ouvrent leur navigateur. À l'évidence, cela nuira aussi quelque peu aux performances, puisque les informations du profil seront téléchargées et le cache sera créé à chaque utilisation. Pour en savoir plus, consultez Mode Éphémère. Veuillez contacter votre spécialiste Chrome Enterprise pour plus d'informations. Certaines entreprises choisissent plutôt de modifier la règle `DefaultCookiesSetting` de sorte qu'aucun cookie ne soit conservé. Nous déconseillons cette méthode, car elle gêne considérablement l'utilisation normale d'Internet. Elle pose en outre un problème de sécurité majeur, puisqu'elle oblige les utilisateurs à saisir leurs mots de passe beaucoup plus souvent, augmentant ainsi le risque d'hameçonnage. Les administrateurs ou les personnes malintentionnés ayant physiquement accès à l'ordinateur pourraient installer un enregistreur de frappes ou un autre logiciel espion, voire un binaire de Chrome falsifié à des fins malveillantes. Une telle mesure traite spécifiquement l'accès de ces personnes aux données de profil stockées sur le disque, mais ne constitue pas une solution exhaustive aux problèmes posés par des administrateurs malveillants. Une solution de portée plus large, dépassant le cadre de Chrome, consisterait à chiffrer le répertoire personnel des utilisateurs.

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

Paramètres concernant les informations stockées sur les appareils de l'entreprise qui permettent d'identifier personnellement l'utilisateur (suite)

Besoin de l'entreprise	Impact sur l'utilisateur	Impact potentiel sur la sécurité	Options et remarques
Je crains qu'une personne ayant physiquement accès à une machine non verrouillée puisse voir les mots de passe d'autres utilisateurs.	● Élevé	● Élevé	Certaines entreprises choisissent de désactiver les fonctionnalités de gestion des mots de passe de Chrome en désactivant la règle `PasswordManagerEnabled`. Nous vous conseillons de maintenir le gestionnaire de mots de passe activé. Ainsi, vos utilisateurs peuvent facilement définir des mots de passe sécurisés sur de nombreux sites, et cela fait partie des mesures les plus importantes que vous puissiez prendre pour leur sécurité. Consultez la section Paramètres concernant les données transmises à Google pour en savoir plus sur les options de gestion des mots de passe. Nous vous recommandons plutôt de définir les règles de verrouillage de l'écran dans le système d'exploitation et de veiller à protéger ce dernier à l'aide de mots de passe sécurisés.

Paramètres concernant les données transmises sur Internet (perte de données)

Besoin de l'entreprise	Impact sur l'utilisateur	Impact potentiel sur la sécurité	Options et remarques
Je souhaite empêcher les importations.	N/A	N/A	À ce jour, Chrome ne propose aucune règle permettant d'empêcher les importations de fichiers. Notez en particulier que la règle `AllowFileSelectionDialogs` ne permet pas d'atteindre cet objectif, car les importations restent possibles par glisser-déposer ou par d'autres mécanismes lorsque cette règle est désactivée.

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

Paramètres concernant les données transmises sur Internet (perte de données) (suite)

Besoin de l'entreprise	Impact sur l'utilisateur	Impact potentiel sur la sécurité	Options et remarques
Je souhaite surveiller ce que font les utilisateurs pour détecter les comportements suspects.	Aucun	Aucun	Vous pouvez surveiller la consommation des ressources du navigateur Chrome, l'état de la connexion, la connectivité, les schémas d'utilisation et le comportement de navigation. Consultez Surveiller l'utilisation du navigateur Chrome sous Windows.
Je souhaite que les données confidentielles ne puissent être affichées que sur l'écran principal de l'ordinateur. Par conséquent, je veux désactiver la fonction Caster de Chrome.	Moyen	Aucun	Modifiez la règle `EnableMediaRouter`.
Je souhaite empêcher des sites Web d'enregistrer un flux vidéo ou audio (par exemple, via WebRTC).	Moyen	Aucun	Vous pouvez utiliser les règles `VideoCaptureAllowed` et `AudioCaptureAllowed` pour empêcher les enregistrements vidéo et audio, en y associant les règles "AllowedUrls" qui permettent de dresser une liste d'autorisation. Certaines entreprises ont entendu dire qu'il faut désactiver WebRTC. Vous ne pouvez pas désactiver totalement la pile WebRTC. Il est préférable de désactiver les capteurs qui présentent un risque pour votre entreprise. Le transfert des outils de visioconférence et de téléphonie vers le Web est en marche. Donc, l'impact de ce phénomène sur vos utilisateurs risque de s'accentuer à l'avenir. Il serait peut-être judicieux de reporter ces décisions d'un an.
Je souhaite empêcher les sites Web d'effectuer des captures d'écran.	Moyen	Aucun	Les versions actuelles de Chrome ne fournissent pas d'API de partage d'écran sans extension. Les sites Web auront sûrement accès à de telles API prochainement, mais elles seront régulées par la règle `VideoCaptureAllowed` mentionnée dans la précédente recommandation. Veuillez contacter votre spécialiste Chrome Enterprise pour vous tenir informé à ce sujet.

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

Paramètres concernant les données transmises sur Internet (perte de données) (suite)

Besoin de l'entreprise	Impact sur l'utilisateur	Impact potentiel sur la sécurité	Options et remarques
#Je souhaite empêcher les sites Web malveillants de demander l'accès en lecture aux ports série, même si cela bloque l'accès de sites Web légitimes.	Moyen	Aucun	Vous pouvez contrôler l'utilisation de l'API File System pour la lecture à l'aide de la règle `DefaultSerialGuardSetting`. Si cette règle est définie sur "3", les sites Web peuvent demander l'accès en lecture aux fichiers et répertoires qui figurent dans le système de fichiers du système d'exploitation hôte via l'API File System. Si cette règle est définie sur "2", l'accès est refusé. Si cette règle n'est pas configurée, les sites Web peuvent demander l'accès. Toutefois, les utilisateurs peuvent modifier ce paramètre.
#Je souhaite empêcher les sites Web malveillants de demander l'accès en lecture aux fichiers et répertoires qui figurent dans le système de fichiers du système d'exploitation hôte via l'API File System, même si cela bloque l'accès de sites Web légitimes.	Moyen	Aucun	Vous pouvez contrôler l'utilisation de l'API File System pour la lecture à l'aide de la règle `DefaultFileSystemReadGuardSetting`. Si cette règle est définie sur "3", les sites Web peuvent demander l'accès en lecture aux fichiers et répertoires qui figurent dans le système de fichiers du système d'exploitation hôte via l'API File System. Si cette règle est définie sur "2", l'accès est refusé. Si cette règle n'est pas configurée, les sites Web peuvent demander l'accès. Toutefois, les utilisateurs peuvent modifier ce paramètre.
#Je souhaite empêcher les sites Web malveillants de demander l'accès aux capteurs et de les utiliser (capteurs de mouvement et de lumière, par exemple), même si cela bloque l'accès de sites Web légitimes.	Moyen	Aucun	Vous pouvez contrôler l'utilisation du paramètre par défaut des capteurs à l'aide de la règle `DefaultSensorsSetting`. Si cette règle est définie sur "1", les sites Web peuvent accéder aux capteurs (de mouvement et de lumière, par exemple) et les utiliser. Si cette règle est définie sur "2", l'accès aux capteurs est refusé. Si cette règle n'est pas configurée, la règle AllowSensors s'applique. Toutefois, les utilisateurs peuvent modifier ce paramètre.

Je souhaite empêcher les sites Web malveillants d'accéder aux appareils USB et Bluetooth, même si cela bloque l'accès de sites Web légitimes.	Moyen	Moyen	`DefaultWebUsbGuardSetting`
			`DefaultWebBluetoothGuardSetting`
			
			Certains sites Web requièrent un accès légitime aux jetons matériels USB ou Bluetooth pour l'authentification multifacteur. La désactivation de l'accès via USB ou Bluetooth peut avoir une incidence sur la sécurité de tels sites Web.

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

Paramètres concernant les données transmises sur Internet (perte de données) (suite)

Besoin de l'entreprise	Impact sur l'utilisateur	Impact potentiel sur la sécurité	Options et remarques
Je souhaite empêcher les sites Web malveillants d'accéder aux données de localisation, même si cela bloque l'accès de sites Web légitimes à la localisation.	Élevé	Faible	Pour désactiver l'accès à la localisation, utilisez `DefaultGeolocationSetting` Cette action est considérée comme très pénalisante en termes d'expérience utilisateur. Elle peut aussi avoir une incidence sur la sécurité, car on peut imaginer que certains sites Web s'appuient sur la localisation pour la sécurité.
Je souhaite empêcher les sites Web tiers de suivre nos utilisateurs sur le Web.	Élevé	Faible	Certaines entreprises désactivent les cookies tiers à l'aide de la règle `BlockThirdPartyCookies`. Cela peut nuire au bon fonctionnement de certains sites Web, par exemple des services Web d'authentification, et donc avoir une incidence sur la sécurité.

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

Paramètres concernant les données transmises à Google

Besoin de l'entreprise	Impact sur l'utilisateur	Impact potentiel sur la sécurité	Options et remarques
Je souhaite empêcher Chrome de divulguer des informations aux serveurs DNS de Google.	N/A	N/A	De nombreux utilisateurs pensent à tort qu'il faut désactiver la règle `BuiltInDnsClientEnabled` pour empêcher Chrome d'utiliser les serveurs DNS de Google. Ils font erreur, car cette option ne s'applique qu'à la pile logicielle DNS côté client, sur le point de terminaison, et n'affecte en rien le choix des serveurs utilisés. La pile DNS Google ne communique jamais avec les serveurs Google, à moins que le point de terminaison soit configuré dès le départ à cette fin. Du point de vue de la confidentialité, les entreprises n'ont aucune raison de modifier cette option.
Je souhaite empêcher que des informations confidentielles sur les plantages et l'utilisation soient envoyées à Google.	Faible	Aucun	Vous pouvez désactiver l'envoi de rapports d'erreur anonymes avec la règle `MetricsReportingEnabled`. Ces métriques sont anonymes. Si vous autorisez leur envoi, Google sera plus à même de comprendre les besoins de votre entreprise et les problèmes de stabilité qu'elle rencontre.
Je ne veux pas que Google soit informé si des logiciels malveillants sont détectés sur les ordinateurs de mon organisation.	Faible	Faible	`ChromeCleanupReportingEnabled` est la règle qui contrôle l'envoi d'informations à Google. Il existe une autre règle, `ChromeCleanupEnabled`, qui détermine si Chrome doit rechercher des logiciels malveillants et inviter les utilisateurs à les supprimer, le cas échéant. Ces deux règles vous permettent de choisir si vous utilisez le service de suppression de logiciels malveillants intégré à Chrome et si Chrome transmet les données relatives aux détections de ce service à Google.
Je souhaite empêcher les utilisateurs d'envoyer des documents confidentiels à des imprimantes cloud via Google.	Moyen	Aucun	Modifiez la règle `CloudPrintSubmitEnabled`. Pour plus d'informations, consultez Qui peut voir les impressions ?
Je souhaite empêcher que le texte des notifications soit transmis via les services Google.	Moyen	Aucun	Certaines entreprises choisissent de désactiver les notifications avec la règle `DefaultNotificationsSetting` pour éviter que le texte des notifications transite par les services de backend Google. Pour plus d'informations, lisez la section concernant les messages push du livre blanc sur la confidentialité dans Google Chrome.

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

Paramètres concernant les données transmises à Google (suite)

Besoin de l'entreprise	Impact sur l'utilisateur	Impact potentiel sur la sécurité	Options et remarques
Je souhaite éviter que Google ait accès à nos mots de passe.	● Moyen	● Moyen	Google vous recommande vivement de maintenir les fonctions de gestion des mots de passe pour vos utilisateurs. Cela leur permet de définir des mots de passe sécurisés qui contribuent largement à votre sécurité globale. Lisez, par exemple, l'article du NCSC à propos des gestionnaires de mots de passe. Lorsque la synchronisation Chrome est désactivée, les mots de passe ne sont pas transmis à Google. Ils ne sont stockés que sur le point de terminaison et chiffrés à l'aide du mot de passe de connexion de l'utilisateur. Ainsi, même les personnes qui ont physiquement accès au disque ne peuvent pas les lire. (Voir les sections précédentes concernant les informations personnelles stockées sur le point de terminaison.) Lorsque la synchronisation Chrome est activée, par défaut, les mots de passe sont stockés dans l'infrastructure Google. Google prend très au sérieux la protection de ces informations, mais pourrait être amené à les divulguer, par exemple pour des raisons juridiques. Lisez le prochain point pour savoir comment faire en sorte que Google n'ait pas du tout accès à ces données. De façon plus générale, Google souhaite que les utilisateurs de la version Enterprise profitent de la meilleure sécurité possible en utilisant un gestionnaire de mots de passe. Si d'autres fonctionnalités ou options pouvaient vous rassurer au point d'activer le gestionnaire de mots de passe, veuillez en faire part à votre spécialiste Google Chrome Enterprise. Certaines entreprises choisissent de désactiver l'option permettant d'importer des mots de passe depuis d'autres navigateurs (règle `ImportSavedPasswords`). Comme pour les gestionnaires de mots de passe en général, nous pensons qu'il est important de faciliter autant que possible l'utilisation de mots de passe sécurisés. Donc, nous recommandons de conserver cette option d'importation.

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

Paramètres concernant les données transmises à Google (suite)

Besoin de l'entreprise	Impact sur l'utilisateur	Impact potentiel sur la sécurité	Options et remarques
Je souhaite éviter que Google ait accès aux données des profils utilisateur, y compris les phrases secrètes et les favoris.	Moyen	Moyen	Vos utilisateurs peuvent définir une phrase secrète de synchronisation, qui chiffre leur profil (mots de passe, favoris, etc.) de sorte qu'il ne soit jamais importé en texte brut. En savoir plus Grâce à la phrase secrète, vos utilisateurs peuvent stocker leurs données Chrome sur le cloud Google et les synchroniser, sans que Google puisse les lire. Ce paramètre impose aux utilisateurs de saisir leur phrase secrète sur les nouveaux appareils et il a des incidences sur la synchronisation de l'historique, ce qui peut les gêner dans leur travail. À ce jour, Chrome ne propose pas de règle permettant d'imposer l'utilisation d'une phrase secrète. Si vous avez d'autres questions, posez-les à votre spécialiste Chrome Enterprise.
Je ne souhaite envoyer aucune donnée à Google, pour des questions de conformité.	Élevé	Élevé	Nous vous recommandons vivement de maintenir la navigation sécurisée pour protéger les utilisateurs contre les logiciels malveillants et l'hameçonnage. La navigation sécurisée de Chrome a accès au contexte qui a orienté l'utilisateur vers une page donnée, ce qui lui permet parfois de fournir une analyse plus pertinente que d'autres produits de sécurité destinés aux entreprises. Renseignez-vous sur les règles liées à la sécurité et à la confidentialité de Chrome. De plus, vous pouvez empêcher la synchronisation des favoris, de l'historique et des mots de passe avec Google grâce à la règle `SyncDisabled`. Cependant, nous vous recommandons vivement de maintenir le gestionnaire de mots de passe. Consultez les deux précédentes lignes du tableau pour connaître les options qui s'offrent à vous dans ce domaine. Chaque entreprise a son avis sur la question. Ainsi, la majorité des entreprises préfère conserver les fonctionnalités qui sont déclenchées par une action explicite de l'utilisateur (par exemple, Google Traduction) et celles qui offrent des avantages évidents en termes de sécurité. Contactez votre spécialiste Chrome Enterprise pour discuter plus avant des données échangées par chaque service et pour trouver les règles les mieux adaptées à votre cas.

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

Gestion et performances

Cette section traite des besoins des entreprises concernant la gestion et les performances de Chrome, qui peuvent avoir trait à la sécurité/confidentialité et à d'autres questions.

Besoin de l'entreprise	Impact sur l'utilisateur	Impact potentiel sur la sécurité	Options et remarques
Je crains que le gestionnaire de mots de passe de Chrome ne parvienne pas à maintenir la synchronisation des mots de passe utilisateur et provoque des escalades à l'assistance.	N/A	N/A	L'équipe Chrome chargée de la sécurité recommande vivement le gestionnaire de mots de passe, car il favorise l'utilisation de mots de passe sécurisés. Notre but est de le rendre aussi simple et transparent que possible. Si vous avez des questions à ce sujet, contactez votre spécialiste Chrome Enterprise.
Je souhaite m'assurer que les utilisateurs ne se feront pas hameçonner leur mot de passe Google Workspace.	● Aucun	● Aucun	Activez l'Alerte mot de passe. Suivez les instructions permettant d'empêcher la réutilisation des mots de passe.
Les tests imposés par mon organisation ne permettent pas de déployer rapidement la dernière version de Chrome.	● Aucun	● Aucun	Chrome propose plusieurs versions disponibles permettant à votre entreprise d'accéder à l'avance aux nouvelles fonctionnalités, aux correctifs de bugs et aux améliorations de la sécurité. Nous vous recommandons d'inscrire certains membres de votre équipe aux versions bêta et en développement pour avoir le temps de tester les nouvelles fonctionnalités et de modifier vos applications professionnelles en conséquence. Cela peut aussi vous donner l'occasion de poser des questions à votre spécialiste Chrome Enterprise avant qu'une modification destructive soit appliquée à la version stable. Nous vous invitons à adopter cette approche plutôt que de retarder les mises à jour et d'exposer ainsi votre organisation à des failles connues. Notez bien que nous développons Chrome selon une approche largement ouverte. Dès qu'un correctif de sécurité est appliqué à la version stable, tous les détails du bug concerné sont accessibles au public. Il est extrêmement important que vos utilisateurs disposent de la version de Chrome la plus récente.

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

Gestion et performances (suite)

Besoin de l'entreprise	Impact sur l'utilisateur	Impact potentiel sur la sécurité	Options et remarques
Je crains que Chrome Cleanup ait un impact sur les performances et agisse en doublon de notre antivirus actuel. Mon organisation souhaite que les dangers soient identifiés et signalés par son propre antivirus, plutôt que par Chrome.	Aucun	Moyen	Certaines entreprises souhaitent désactiver Chrome Cleanup pour des questions de performances (en particulier dans les environnements VDI) ou pour que les logiciels malveillants soient détectés par le logiciel antivirus de l'entreprise et que les alertes passent par leurs outils de gestion des informations et des événements de sécurité (SIEM, Security information and event management) et par d'autres processus qui leur sont propres. Sachez que cela a un impact sur la sécurité. L'outil Chrome Cleanup recherche les logiciels indésirables, plutôt que les virus, et peut donc détecter et supprimer différents logiciels. Cela dit, vous pouvez le désactiver en modifiant la règle `ChromeCleanupEnabled`. Remarque : Si vous souhaitez simplement empêcher Chrome Cleanup de transmettre ses résultats à Google, il existe d'autres moyens plus adaptés (voir la section "Je ne veux pas que Google soit informé si des logiciels malveillants sont détectés sur les ordinateurs de mon organisation.").
L'intranet de mon organisation n'utilise pas encore HTTPS, et les avertissements liés à la sécurité effraient les utilisateurs.	Aucun	Moyen	Vous pouvez désactiver l'affichage de ces avertissements avec la règle `OverrideSecurityRestrictionsOnInsecureOrigin`. Cependant, passez au protocole HTTPS dès que possible, car cette règle sera probablement appelée à disparaître prochainement.
Je veux m'assurer de pouvoir réaliser un audit complet si je dois enquêter rétrospectivement sur une violation.	Faible	Aucun	Normalement, les utilisateurs peuvent désactiver l'enregistrement de l'historique de navigation. Vous pouvez leur ôter cette possibilité en modifiant la règle `SavingBrowserHistoryDisabled`. Vous pouvez aussi désactiver le mode navigation privée à l'aide de la règle `IncognitoModeAvailability`.
Je souhaite que les utilisateurs adoptent le gestionnaire de mots de passe approuvé par l'entreprise, et non celui qui est intégré dans Chrome.	Faible	Faible	Vous prenez la bonne décision en fournissant un gestionnaire de mots de passe à vos utilisateurs. Pour désactiver le gestionnaire de mots de passe intégré, modifiez la règle `PasswordManagerEnabled`. Nous vous conseillons de n'appliquer cette règle qu'à votre profil d'entreprise de sorte que les utilisateurs puissent tout de même profiter du gestionnaire de mots de passe Chrome lorsqu'ils se connectent avec leur profil Chrome personnel.

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

Gestion et performances (suite)

Besoin de l'entreprise	Impact sur l'utilisateur	Impact potentiel sur la sécurité	Options et remarques
Je souhaite empêcher les utilisateurs de visiter certains sites en raison de la politique de l'entreprise.	Moyen	Aucun	Il existe pour cela des règles permettant de définir des listes d'autorisation et de blocage. Consultez Autoriser ou bloquer l'accès à des sites Web.
#Je souhaite que le comportement de Chrome soit prévisible et qu'il n'évolue qu'aux changements de version.	Moyen	Aucun	Les variantes sont un moyen de proposer des modifications de Google Chrome sans créer de nouvelles versions du navigateur, en activant ou en désactivant des fonctionnalités déjà disponibles. Si vous définissez la règle `ChromeVariations` sur `VariationsEnabled (valeur "0")` ou si vous ne la configurez pas, toutes les variantes sont appliquées au navigateur. Il n'est pas conseillé de désactiver le framework des variantes Chrome. Cette action pourrait empêcher Google de fournir rapidement des correctifs de sécurité essentiels, et augmenter considérablement le risque de problèmes de sécurité et de compatibilité dans votre organisation.
Je souhaite qu'à chaque démarrage le navigateur affiche une page de connexion centrale ou une autre page de l'entreprise pour que les utilisateurs acceptent la politique de l'organisation ou voient des informations importantes la concernant.	Moyen	Aucun	Envisagez les règles `RestoreOnStartupURLs`, `HomepageIsNewTabPage`, `NewTabPageLocation` et `HomepageLocation`.
Je souhaite que les utilisateurs n'aient pas accès au mode navigation privée, car je crains qu'il les incite à consulter des sites Web potentiellement inappropriés dans un environnement professionnel.	Moyen	Aucun	Modifiez la règle `IncognitoModeAvailability`.

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

Gestion et performances (suite)

Besoin de l'entreprise	Impact sur l'utilisateur	Impact potentiel sur la sécurité	Options et remarques
Mes points de terminaison utilisent un logiciel incompatible avec la pile DNS de Chrome.	Moyen	Moyen	Chrome possède une pile DNS intégrée que vous pouvez désactiver avec la règle `BuiltInDnsClientEnabled`. (Cette règle n'affecte que la pile logicielle DNS utilisée, et non pas les serveurs DNS eux-mêmes.) Si un logiciel installé sur vos points de terminaison modifie le comportement normal des API DNS, vous devrez peut-être configurer Chrome de sorte qu'il utilise la pile DNS du système. Cela peut avoir un impact sur la vitesse et la réactivité des pages Web, ainsi que sur la sécurité, car cela empêche Chrome de renforcer la connexion avec DNS sur TLS ou avec de futurs protocoles plus sécurisés.
Je dois analyser le trafic Internet à l'aide de boîtiers intermédiaires.	Moyen	Moyen	Vous allez devoir installer un certificat racine sur chaque point de terminaison. Google prend des mesures extensives pour vérifier la sécurité des certificats utilisés sur Internet (par exemple, concernant la transparence des certificats), mais n'est évidemment pas en mesure de contrôler le bon usage des certificats de votre entreprise. Consultez la section "Mon organisation utilise ses propres certificats racines de confiance sur ses points de terminaison pour authentifier les serveurs de l'entreprise. Si des pirates informatiques volent la clé privée de ces certificats racines de confiance, je dois être en mesure de les révoquer." qui donne des conseils permettant de limiter ces risques. Google déconseille l'utilisation de versions antérieures de TLS pour des raisons de compatibilité avec des boîtiers intermédiaires plus anciens. Les versions de TLS antérieures à la 1.2 comportent des failles connues, et l'architecture de TLS 1.3 vous protège de différentes vulnérabilités inconnues.

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

Gestion et performances (suite)

Besoin de l'entreprise	Impact sur l'utilisateur	Impact potentiel sur la sécurité	Options et remarques
Je dois analyser le comportement des utilisateurs dans Chrome à l'aide d'un produit tiers.	Moyen	Aucun	Vous pouvez installer d'office des extensions de sécurité tierces à l'aide de la règle `ExtensionInstallForcelist`. Sachez toutefois que cela peut autoriser ces extensions à accéder à l'historique de navigation, aux données utilisateur et aux chargements de page. Il est préférable d'utiliser cette option plutôt que d'autoriser l'injection d'un code tiers dans les processus du navigateur en modifiant la règle `ThirdPartyBlockingEnabled`. Selon l'expérience de notre équipe Chrome, les entreprises qui injectent un code tiers s'exposent à un risque accru, car elles brisent ainsi certaines des protections intégrées dans Chrome.
Mon organisation applique des règles par utilisateur à l'aide d'une configuration Google Cloud. Je souhaite m'assurer que les utilisateurs sont toujours soumis à ces paramètres en leur imposant de se connecter à leur profil professionnel dans Chrome.	Élevé	Aucun	Obligez les utilisateurs à se connecter au navigateur Chrome avec un profil professionnel (en savoir plus). Les utilisateurs ne pourront pas se connecter à Chrome avec leur profil personnel pour synchroniser leurs propres favoris, mots de passe, etc. Si cela vous convient mieux, vous pouvez aussi appliquer des paramètres à l'ensemble des appareils avec la gestion cloud du navigateur Chrome ou avec la stratégie de groupe Windows.

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.

Gérer Chrome

En tant qu'administrateur informatique, vous pouvez déployer Chrome pour des utilisateurs sur différentes plates-formes, puis utiliser les centaines de règles à votre disposition pour contrôler l'utilisation de Chrome.

Débuter dans la gestion Chrome

BeyondCorp Enterprise

BeyondCorp est un modèle de sécurité zéro confiance façonné par Google qui transfère le contrôle des accès du périmètre aux appareils et utilisateurs individuels. Cela permet aux employés de travailler de façon sécurisée où qu'ils se trouvent sans avoir à recourir à un VPN classique. Avec BeyondCorp Enterprise, les utilisateurs peuvent adopter une approche zéro confiance basée sur des principes également appliqués chez Google et gérer ainsi l'accès à leurs applications SaaS hébergées sur Google Cloud, sur d'autres clouds ou sur site. BeyondCorp Enterprise inclut de nouveaux services de protection contre les menaces et les violations de données. Les utilisateurs bénéficient d'un niveau de sécurité supplémentaire intégré directement dans le navigateur Chrome et qui ne requiert pas d'agent.

Notre nouveau livre blanc intitulé "Secure access to SaaS applications with BeyondCorp Enterprise" (Accès sécurisé aux applications SaaS avec BeyondCorp Enterprise) destiné aux responsables informatiques présente divers scénarios courants et des conseils permettant de les traiter. Comme pour tout nouveau déploiement, les organisations sont confrontées à un certain nombre de questions de sécurité :

- Comment gérer l'accès zéro confiance aux applications SaaS concernées ?
- Comment empêcher les fuites de données sensibles associées aux applications SaaS ?
- Comment prévenir les transferts de logiciels malveillants et les mouvements latéraux via les applications concernées ?
- Comment prévenir l'accès aux URL d'hameçonnage insérées dans les contenus de l'application ?

Nous traitons ces questions de façon détaillée, ainsi que plusieurs autres scénarios, dans le livre blanc. Nous vous proposons de lire ce livre blanc et d'en apprendre davantage sur BeyondCorp Enterprise avec notre webinaire de présentation à la demande ou sur notre page produit.

Autres ressources

Voici d'autres ressources qui vous permettront de gérer Chrome dans votre organisation :

Guide de déploiement du navigateur Chrome (Windows)
Liste des règles Chrome Enterprise
Notes de version de Chrome Enterprise
Centre d'aide Chrome Enterprise
Gérer les extensions dans votre entreprise

© 2021 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, États-Unis.