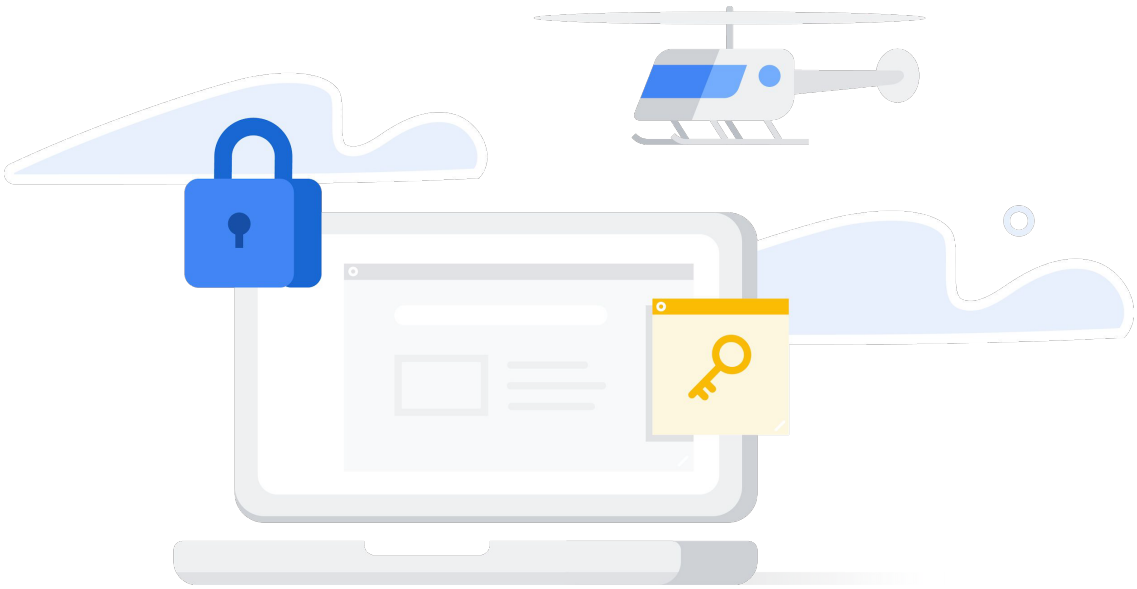
chrome enterprise

Le navigateur en première ligne pour protéger les points de terminaison contre les attaques de sécurité

Comment le navigateur Chrome peut-il jouer un rôle central dans votre stratégie de sécurité en entreprise ?



Les navigateurs comme outils stratégiques de sécurité

Les navigateurs sont souvent sous-estimés et considérés comme de simples portails d'accès à Internet. Ils sont cependant devenus de réelles plates-formes sophistiquées. Ils compilent et exécutent des scripts et du code. Ils permettent aux utilisateurs d'effectuer des recherches et de naviguer facilement sur le Web ainsi que dans des applications. Ils offrent des expériences immersives et complètes, alliant texte, images, audio, vidéo et réalité virtuelle. Et ils proposent de nombreuses applications et extensions parfaitement intégrées.

Les navigateurs disposent déjà de nombreuses fonctionnalités pour renforcer la sécurité du réseau et des points de terminaison. Ils bénéficient, en fin de compte, d'une position unique pour devenir un élément stratégique de la sécurité des entreprises. Point de rencontre entre le Web, les utilisateurs et les applications, ils sont le lieu idéal pour atteindre plusieurs objectifs :

Interagir avec les utilisateurs en temps réel pour prévenir les comportements dangereux

Appliquer des règles de sécurité centrées sur les utilisateurs aux points de terminaison

Gérer la sécurité des points de terminaison sur les différents appareils et systèmes d'exploitation de manière simple et cohérente

Dans ce document, vous découvrirez comment les navigateurs peuvent remplir ces trois fonctions à travers des exemples s'appuyant sur le navigateur Google Chrome.

Prévenir les comportements dangereux des utilisateurs

Les entreprises ont investi des milliards d'euros pour déployer de puissants outils de sécurité visant à repérer les logiciels malveillants et les indicateurs de compromission sur leurs systèmes et leur réseau. Malheureusement, les pirates informatiques peuvent contourner la plupart de ces outils en exploitant le maillon faible de la sécurité des entreprises : les utilisateurs d'ordinateurs et de smartphones, tels que les employés, les prestataires, les clients et les fournisseurs.

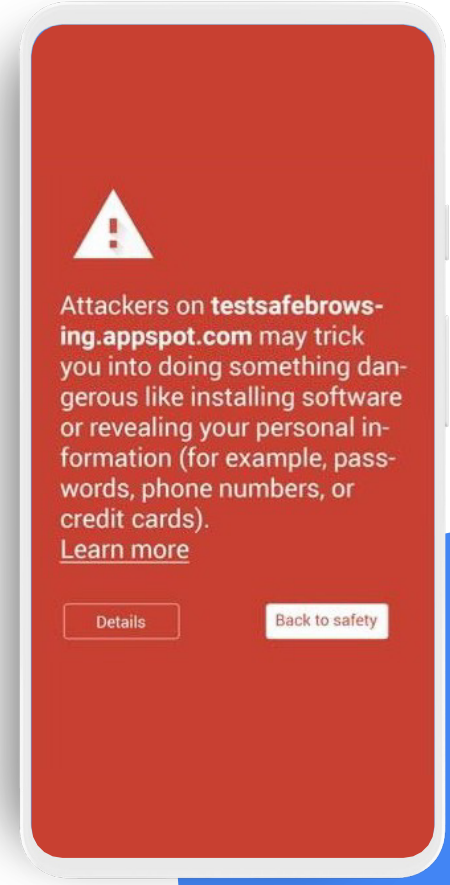
De nos jours, les pirates informatiques font preuve de plus en plus d'ingéniosité pour créer des attaques par hameçonnage ou ingénierie sociale qui attireront les utilisateurs sur des sites Web qu'ils contrôlent et les inciteront à télécharger des fichiers malveillants, à saisir leurs identifiants sur des formulaires, voire à transférer de l'argent sur des comptes bancaires inconnus. Même les meilleurs programmes de sensibilisation à la sécurité ne peuvent que réduire, et non éliminer, l'éventualité de telles attaques.

Pour éviter que les utilisateurs tombent dans ces pièges, les navigateurs peuvent prévenir les comportements dangereux. Le navigateur Chrome offre de très bons exemples de fonctionnalités qui avertissent les utilisateurs en cas d'attaque par hameçonnage ou ingénierie sociale potentielle et qui leur indiquent comment réagir pour rester en sécurité.

La navigation sécurisée : une protection en temps réel contre l'hameçonnage et les logiciels malveillants

La navigation sécurisée dans Chrome empêche les utilisateurs d'accéder à des sites malveillants ou infectés sur le Web.

La navigation sécurisée de Google analyse le contenu de milliards de pages Web et tient à jour une liste des sites Web à risque. Il peut s'agir de sites créés par des pirates informatiques ou de sites Web légitimes qui ont été compromis.
Google s'appuie sur plusieurs critères pour les identifier : la présence de logiciels malveillants, la participation à de précédentes attaques par hameçonnage ou ingénierie sociale et la présence de liens ou de code qui redirigent les utilisateurs vers un site pirate. Les tentatives de se faire passer pour un autre site, une organisation connue ou une autre entité, ainsi que la présence de texte ou de formulaires qui demandent aux utilisateurs de renseigner leurs mots de passe, d'appeler un numéro d'assistance technique ou de télécharger un logiciel sont également prises en compte. Le service de navigation sécurisée recense actuellement plus de 21 000 sites d'attaque par logiciel malveillant et 1,8 million de sites d'hameçonnage, et envoie plus de 3 millions d'avertissements aux utilisateurs chaque jour.



> Chaque fois qu'un utilisateur tente d'accéder à une page Web qui figure sur la liste de la navigation sécurisée, le navigateur Chrome affiche un avertissement qui lui explique le risque et l'invite à revenir en lieu sûr (voir l'illustration). Chrome a affiché plus d'un milliard d'avertissements de ce type en 2019.

La navigation sécurisée est activée par défaut et la liste est actualisée toutes les 30 minutes pour tenir compte des nouveaux sites d'hameçonnage ou contenant des logiciels malveillants découverts. Si un administrateur ou un utilisateur final active la navigation sécurisée avec protection renforcée,
le navigateur Chrome inspectera chaque page Web en temps réel. Cette fonctionnalité vise à protéger les utilisateurs des pirates informatiques qui créent de nouvelles URL à quelques minutes d'intervalle pour échapper aux outils de sécurité s'appuyant sur des listes de blocage d'URL classiques.
Les équipes informatiques peuvent définir une règle afin de configurer la navigation sécurisée pour l'ensemble de leur organisation.

D'après les données de Google, les utilisateurs qui se servent de cette fonctionnalité voient l'efficacité de leur protection contre l'hameçonnage augmenter de 30 à 50 %.

La navigation sécurisée protège également les utilisateurs contre les extensions et les logiciels malveillants. Lorsque le navigateur est lancé, ou lorsque la liste de la navigation sécurisée est actualisée, Chrome scanne les extensions qui y sont installées et les compare aux extensions malveillantes figurant sur la liste. Si une correspondance est trouvée, Chrome désactive l'extension, avertit l'utilisateur et lui présente éventuellement des options pour la supprimer ou la réactiver.

De la même manière, lorsqu'un utilisateur télécharge un fichier, le navigateur Chrome le vérifie en parallèle d'une liste de types de fichiers potentiellement dangereux (les exécutables ou les formats de documents souvent utilisés à des fins malveillantes, par exemple). Si la sécurité du fichier ne peut pas être confirmée, le navigateur Chrome envoie l'information aux serveurs Google afin qu'ils déterminent s'il est sûr. Si ce n'est pas le cas, un avertissement s'affiche1.

Il est possible d'activer la navigation sécurisée avec protection renforcée pour augmenter significativement la protection contre les sites Web et les téléchargements malveillants. Chrome transmet des données en temps réel à cette fonctionnalité afin de protéger les utilisateurs de façon proactive contre les sites dangereux. Lorsqu'un utilisateur est connecté, Chrome ainsi que les autres applications Google utilisées (Gmail, Drive, etc.) sont plus à même de le protéger, car elles profitent d'une vue d'ensemble sur les menaces rencontrées sur le Web et sur les attaques à l'encontre de ce compte Google. La navigation sécurisée avec protection renforcée intègre ainsi l'intelligence des outils de sécurité de pointe de Google au navigateur.

La navigation sécurisée protège aussi les utilisateurs lorsqu'ils se servent des outils de la recherche Google, de Gmail et de smartphones Android pour effectuer diverses tâches.

[1] Pour en savoir plus sur la navigation sécurisée Google, lisez le rapport Google Transparence des informations et le livre blanc sur la confidentialité dans Google Chrome.

Protection des mots de passe avancée

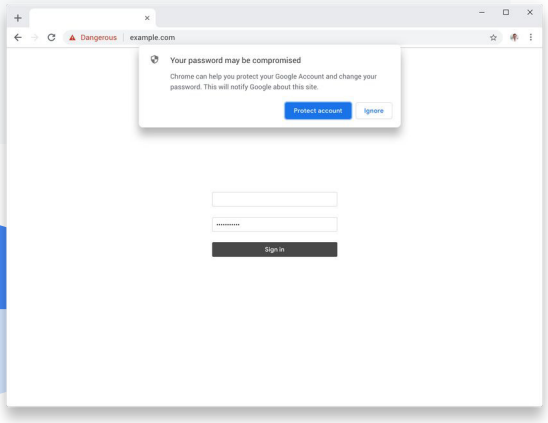
Les mots de passe peuvent permettre aux acteurs malveillants d'accéder aux réseaux, aux applications et aux données des entreprises. Les risques liés aux mots de passe sont d'autant plus importants que de nombreux utilisateurs les réutilisent pour plusieurs comptes et ne les changent pas une fois qu'ils ont été compromis. D'après une étude approfondie sur ces pratiques, 52 % des utilisateurs choisissent le même mot de passe pour deux comptes ou plus,
ou y apportent des modifications mineures que des algorithmes entraînés peuvent prévoir. Par ailleurs, plus de 70 % des utilisateurs interrogés se servaient toujours des mêmes mots de passe plus d'un an après une violation de données et 40 % utilisaient toujours des mots de passe compromis après trois ans2.

> Chrome propose plusieurs fonctionnalités pour éviter l'utilisation d'un même mot de passe pour plusieurs comptes ou de mots de passe qui ont été compromis lors d'une violation de données.

La **protection prédictive contre l'hameçonnage** avertit les utilisateurs s'ils saisissent, sur un site d'hameçonnage potentiel, un mot de passe stocké dans le gestionnaire de mots de passe intégré à Chrome. Elle évite ainsi que des pirates informatiques capturent des identifiants professionnels et s'en servent pour s'introduire dans l'entreprise (ou les vendent à d'autres acteurs malveillants).

Alerte mot de passe est une règle du navigateur Chrome que toutes les entreprises peuvent appliquer. Si elle est activée, le navigateur Chrome détecte lorsqu'un mot de passe professionnel est réutilisé sur un site non approuvé. Elle avertit alors l'utilisateur, l'informe du non-respect des règles et l'invite à réinitialiser le mot de passe (voir l'illustration)[3].

Les utilisateurs finaux peuvent aussi être informés des éventuels problèmes liés à leurs mots de passe. Lorsqu'ils saisissent leurs identifiants sur un site Web, la fonctionnalité **Check-up Mots de passe** les avertit si leur nom d'utilisateur ou leur mot de passe a été compromis lors d'une violation de données et, le cas échéant, leur suggère de changer le mot de passe de tous les comptes liés à ces identifiants.
Cette fonctionnalité leur permet également de vérifier à tout moment si leurs mots de passe ont été compromis lors d'une violation de données, s'ils sont faibles ou s'ils sont utilisés sur plusieurs comptes (voir l'illustration).



[2] "The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services", Chun Wang, Steve T.K. Jan, Hang Hu, Douglas Bossart, Gang Wang, département d'informatique, Virginia Tech : https://people.cs.vt.edu/gangwang/pass.pdf.
[3] Pour en savoir plus sur Alerte mot de passe, consultez Principes de base pour les administrateurs : Protection des identifiants de votre entreprise avec Alerte mot de passe ainsi que Questions fréquentes sur la protection contre l'hameçonnage avec Alerte mot de passe.

Appliquer des règles sur les différents points de terminaison

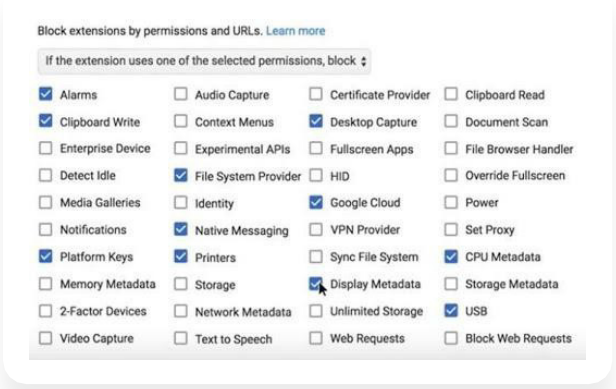
Les règles de sécurité visent à empêcher les utilisateurs d'effectuer des actions dangereuses telles qu'accéder à des sites infectés ou télécharger et installer des applications malveillantes sur les boutiques en ligne. Dans ces deux cas, les navigateurs sont idéalement placés pour appliquer des règles de manière uniforme sur de nombreux types de points de terminaison.

Si certaines règles peuvent être définies de manière individuelle pour les différents utilisateurs du navigateur, nous nous concentrerons ici sur des exemples de règles pouvant être gérées de façon centralisée avec la gestion cloud du navigateur Chrome ou par le biais d'une stratégie de groupe et appliquées à des points de terminaison gérés dotés du navigateur Chrome. Avec la gestion cloud du navigateur Chrome, il est possible d'appliquer des règles à la fois sur le réseau d'une entreprise et en dehors, ce qui en fait l'outil idéal pour des équipes en télétravail.

Listes de blocage et d'autorisation des URL

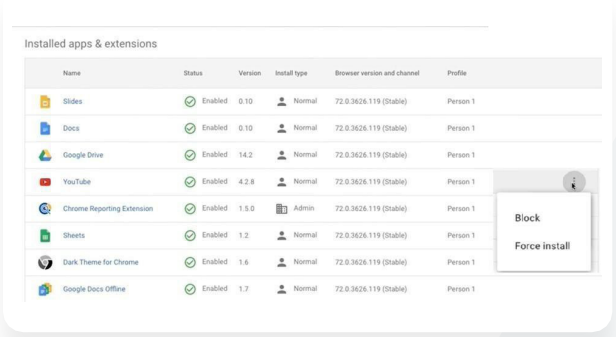
Les administrateurs peuvent dresser des listes de blocage pour empêcher les utilisateurs d'accéder à des sites dangereux connus ou à des URL inappropriées. À l'inverse, ils peuvent créer des listes d'autorisation pour restreindre l'accès des utilisateurs aux seules URL approuvées. Les listes de blocage et d'autorisation peuvent être appliquées de manière sélective aux membres d'unités organisationnelles précises ou à des groupes d'utilisateurs.

Contrôle des applications et des extensions



Les applications et les extensions téléchargeables sont des éléments centraux de l'expérience utilisateur. Elles améliorent le fonctionnement des navigateurs, offrent des fonctionnalités particulières et permettent d'accéder à des données, des documents et des ressources informatiques. Cependant, de nombreux pirates informatiques tentent d'inciter les utilisateurs à télécharger et installer des logiciels malveillants en les faisant passer pour des applications utiles.

La gestion cloud du navigateur Chrome permet aux administrateurs de créer et d'appliquer des listes de blocage répertoriant les applications et les extensions dangereuses connues. Ils peuvent aussi dresser une liste d'autorisation recensant les seules applications et extensions approuvées que les utilisateurs peuvent télécharger.



Il est par ailleurs possible de bloquer toute application ou extension qui nécessite des autorisations précises, par exemple l'autorisation d'accéder aux imprimantes ou aux ports USB, d'écrire dans le presse-papiers, d'enregistrer un flux vidéo ou audio, ou d'émettre des requêtes via le Web (voir l'illustration). Ces autorisations peuvent en effet poser problème en cas d'extension malveillante.

Les administrateurs peuvent savoir quelles applications et extensions sont installées sur chaque point de terminaison géré de leur entreprise. Ils sont en mesure d'en bloquer ou d'en installer d'office (voir l'illustration), ce qui leur permet d'empêcher l'exécution d'applications et d'extensions suspectes ou non professionnelles, et de s'assurer que tous les systèmes sont dotés de celles qui sont indispensables d'un point de vue sécuritaire ou opérationnel.
Des informations supplémentaires sur les extensions peuvent être exportées à l'aide d'une API afin d'être analysées plus en détail ou d'être utilisées pour préparer les rapports de sécurité et de conformité.

Réduire la surface d'attaque

Pour éviter que des applications Web et des extensions malveillantes utilisent les ressources des points de terminaison, les administrateurs peuvent par exemple leur interdire l'accès aux microphones, aux caméras et aux périphériques USB ou empêcher l'exécution de JavaScript.

Appliquer l'authentification à deux facteurs

L'authentification à deux facteurs protège les systèmes et les données même lorsque des mots de passe ont été compromis. Le navigateur Chrome permet aux administrateurs d'imposer son utilisation et de choisir parmi plusieurs méthodes d'authentification, par exemple saisir un code dans un champ de texte, appuyer sur une invite sur un smartphone ou utiliser une clé de sécurité physique à insérer dans le port USB d'un ordinateur portable ou d'un appareil.

Contrôler les anciens navigateurs

Certains utilisateurs ont toujours besoin d'accéder à d'anciennes applications Web basées sur des plug-ins ou ActiveX qui ne sont pas prises en charge par les navigateurs récents. Cependant, autoriser l'utilisation d'anciens navigateurs non sécurisés pour ces applications pose non seulement des problèmes de performances et de compatibilité, mais augmente également le risque de voir ses points de terminaison compromis et d'être victime de violations de données.

La fonctionnalité Legacy Browser Support intégrée à Chrome atténue ces problèmes et permet de diminuer le temps que les utilisateurs passent sur des navigateurs moins sûrs. Les administrateurs peuvent définir des règles qui imposent l'utilisation de Chrome pour l'accès aux applications Web de l'entreprise et à des sites externes actualisés, et d'autres qui limitent l'utilisation d'un ancien navigateur à des applications précises pour lesquelles cela s'avère indispensable. Cette fonctionnalité permet aux utilisateurs de passer facilement d'un navigateur à l'autre au besoin.

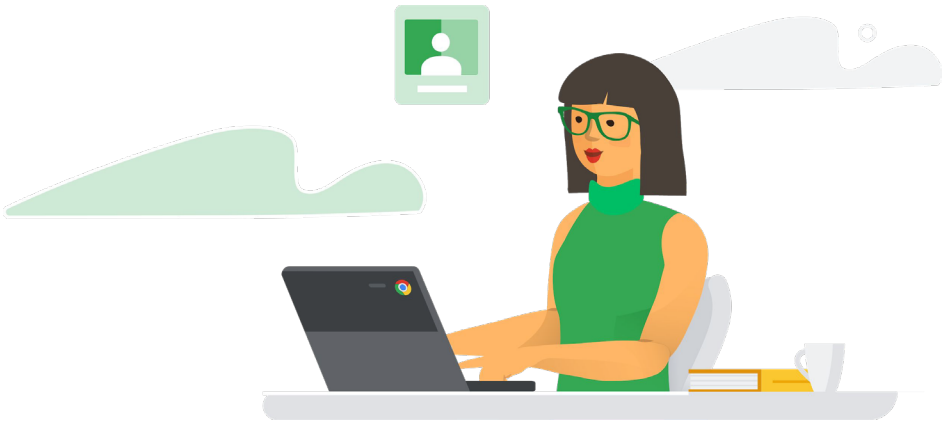
Favoriser la confidentialité

De nos jours, de nombreux points de terminaison sont partagés : systèmes temporaires ou de prêt pour les invités et les prestataires, appareils publics tels que les kiosques, stations de travail temporaires pour les collaborateurs mobiles, et appareils à usage à la fois professionnel et personnel prêtés à des proches en dehors du bureau. Dans de telles circonstances, il est primordial que les utilisateurs qui partagent un même appareil ne puissent pas voir leurs activités respectives et il est bien souvent souhaitable que toutes les traces de ces activités soient supprimées à la fin de chaque session d'utilisation.

> Sur les systèmes partagés dotés du navigateur Chrome, les administrateurs peuvent appliquer des modes Invité et Éphémère. Les utilisateurs ne peuvent alors ni voir, ni modifier les informations liées au profil Chrome des autres utilisateurs.

En mode Invité, les utilisateurs partent d'un écran vierge, sans favoris ni applications ou extensions activées. À la fin de la session, le navigateur supprime les données de navigation telles que les URL visitées, le texte des pages mises en cache, les instantanés des pages consultées, les traces des fichiers téléchargés et les adresses IP des pages faisant l'objet de liens sur les sites Web consultés.

En mode Éphémère, les utilisateurs peuvent activer la synchronisation Chrome pour accéder à leurs favoris (y compris les favoris professionnels), à leur historique de navigation, à leurs applications et extensions, aux pages de l'intranet de l'entreprise et à leur messagerie Web professionnelle. Ils peuvent également profiter de fonctionnalités comme les règles cloud ou le stockage de mots de passe. Cependant, comme pour le mode Invité, toutes les traces de l'activité de navigation sont supprimées à la fin d'une session.



Gérer la sécurité des points de terminaison sur les différents appareils et systèmes d'exploitation

La gestion des points de terminaison est une tâche complexe pour les équipes informatiques et de sécurité. Généralement, les administrateurs créent différentes règles et déploient plusieurs agents pour les divers types de points de terminaison. La mise à jour des outils de sécurité et l'application des correctifs sont des tâches fastidieuses, mais ne pas les faire laisse les points de terminaison vulnérables aux nouvelles attaques.

Avec un navigateur comme Chrome, en revanche, les administrateurs peuvent créer un ensemble de règles et l'appliquer à tous les points de terminaison, sans avoir à déployer plusieurs agents ni à s'occuper des mises à jour et des correctifs. Les utilisateurs, quant à eux, profitent de règles cohérentes lorsqu'ils passent d'un appareil à un autre.

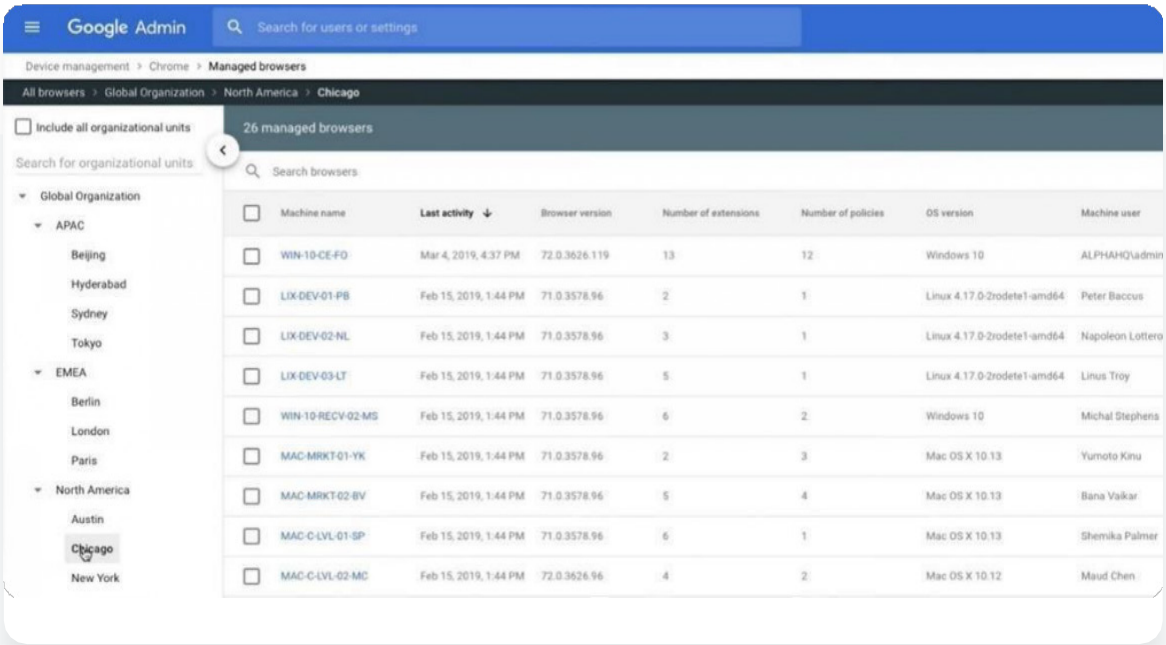
Un seul outil pour tous les systèmes d'exploitation d'ordinateur

La gestion cloud du navigateur Chrome permet aux administrateurs de définir et de gérer les règles de sécurité à partir d'une seule console pour les navigateurs Chrome de tous les points de terminaison sous Windows, macOS, Linux et Chrome OS.

> Nous traitons des informations sensibles, donc, la sécurité est primordiale. Le navigateur Chrome nous aide à gérer la sécurité à chaque point de contact, sur chaque ordinateur portable et pour chaque utilisateur dans notre entreprise."
>
> **Directeur de la technologie,**
> **The Climate Corporation**

Visibilité

La gestion cloud du navigateur Chrome offre une vue d'ensemble de tous les appareils gérés installés dans l'entreprise, y compris une visibilité sur leur système d'exploitation, la version du navigateur Chrome, les extensions installées et le nombre de règles appliquées (voir l'illustration).



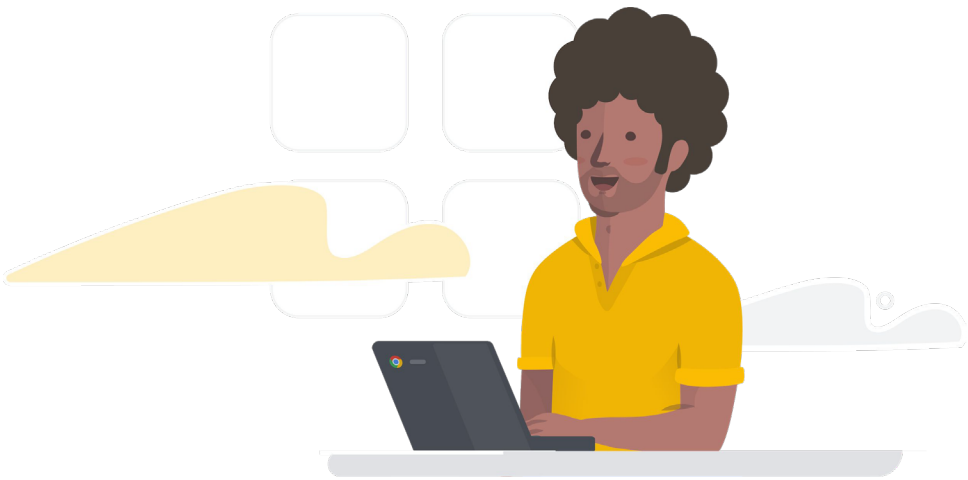
Gestion simplifiée

Avec la gestion cloud du navigateur Chrome, les administrateurs peuvent rapidement créer et déployer des centaines de règles en ce qui concerne la sécurité, les extensions, l'accessibilité, le contenu, l'affichage, l'authentification, la compatibilité avec les anciens navigateurs, les paramètres des réseaux, la gestion des mots de passe, la création de rapports et bien d'autres éléments.

Les navigateurs Chrome peuvent être inscrits à l'aide d'une stratégie de groupe Windows, d'un fichier de préférences sur Mac ou en exécutant un fichier directement sur l'appareil. Les administrateurs ont la possibilité d'appliquer les règles en fonction des rôles utilisateur définis dans Active Directory et de gérer les navigateurs par groupes selon l'emplacement, le type d'appareil ou d'autres facteurs. Ils n'ont pas à se soucier de déployer des agents sur tous les points de terminaison, car les règles modifiées sont transmises aux navigateurs de manière automatique. Certaines tâches de gestion des navigateurs peuvent être déléguées aux professionnels de l'informatique de l'ensemble de l'entreprise pour soulager les administrateurs.

Intégration avec d'autres outils de sécurité

La gestion cloud du navigateur Chrome interagit avec vos autres solutions de gestion et de sécurité. Via des API, elle échange des informations avec des produits tels que VMware Workspace One, Intune et JAMF, ainsi qu'avec les systèmes SIEM et d'autres outils de sécurité. Des modèles de stratégies de groupe sont également disponibles pour les entreprises qui préfèrent les outils de gestion traditionnels de Windows.



Intégrer la sécurité au navigateur

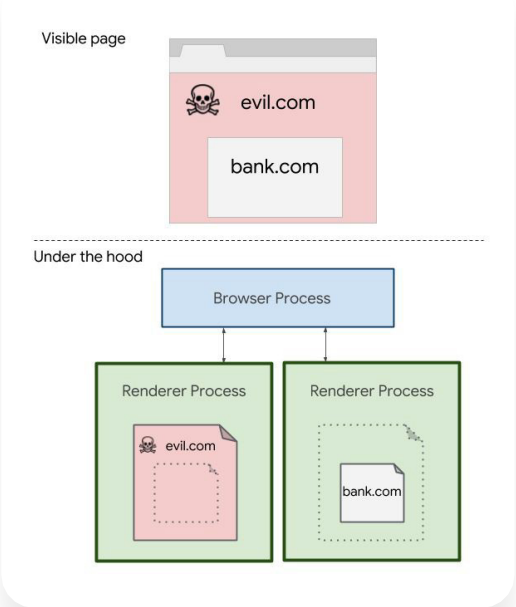
Bien entendu, pour qu'il soit un outil de sécurité efficace, le navigateur lui-même doit être sécurisé.

Bac à sable et isolation de sites

Le navigateur Chrome applique un système de bac à sable. Plutôt que de gérer sa charge de travail comme un seul grand processus de navigateur, Chrome la divise en processus distincts et limite la capacité de chaque processus à accéder à un autre ainsi qu'aux autres ressources du système. Il exécute également chaque application et extension dans son propre processus.

Par exemple, si une page HTML comprend plusieurs éléments JavaScript, le navigateur Chrome exécutera le rendu HTML dans un processus et chaque élément JavaScript dans un processus distinct qui lui est propre. Les jetons d'accès sont changés pour les processus, de sorte que du code malveillant ne puisse pas affecter ou planter les autres processus, modifier les fichiers ou les clés de registre, écrire dans le presse-papiers, capturer les données de l'écran, enregistrer les frappes ou effectuer d'autres actions dangereuses. Cette technique empêche de nombreux pirates informatiques de perturber les applications, d'installer des logiciels malveillants persistants, d'accéder à des données confidentielles sur le disque dur ou de capturer les identifiants des utilisateurs.

Le navigateur Chrome va encore plus loin dans la protection sur les systèmes sous Windows, Mac, Linux et Chrome OS avec une fonctionnalité appelée "isolation de sites". Une seule page Web peut renfermer du contenu issu de plusieurs sites. Avec l'isolation de sites, le contenu de chacun de ces sites Web est exécuté dans son propre processus (voir l'illustration). Les iFrames inter-sites ne font pas exception et sont exécutés dans des processus distincts de celui de la page parente.



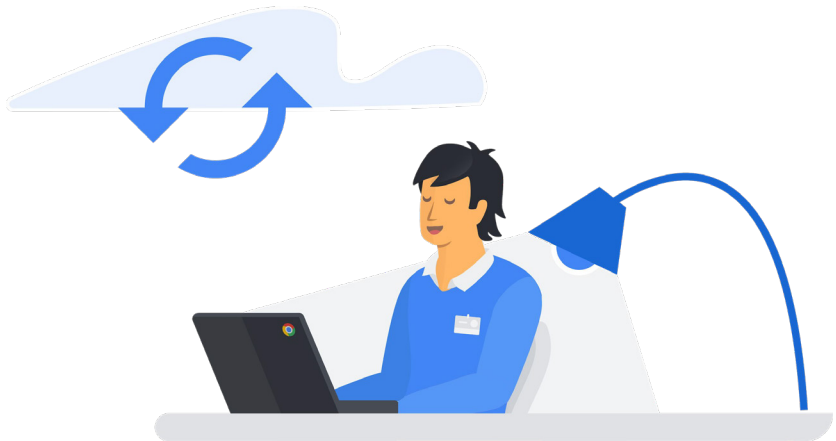
L'isolation de sites contribue à limiter les conséquences des attaques par exécution de code arbitraire ainsi que des attaques par canal auxiliaire d'exécution spéculative comme Spectre et Meltdown. Si un pirate informatique parvient à envoyer du code malveillant au navigateur à partir d'un site Web compromis (tel que evil.com sur l'illustration),
ce code ne pourra pas voler d'informations sur les autres sites (comme bank.com sur l'illustration), car leur code est exécuté dans des processus protégés distincts.

Mises à jour fréquentes et automatisées

Pour protéger ses équipes, il est essentiel de s'assurer que leurs navigateurs sont à jour. Or, cela exige de pouvoir y appliquer les mises à jour et les correctifs rapidement et facilement, sans avoir à déployer trop d'efforts.

Chrome est optimisé dans ce but. Chaque navigateur vérifie à intervalles réguliers si des mises à jour de sécurité sont disponibles et les applique automatiquement. L'utilisateur n'a rien à faire. Par ailleurs, Google distribue les correctifs rapidement. Le délai habituel entre la correction d'un bug de sécurité dans une bibliothèque Open Source et le moment où le correctif est déployé a été réduit à 20 jours seulement, ce qui est inférieur à d'autres navigateurs répandus.

> La gestion des failles et l'application des correctifs représentent un travail considérable dans notre entreprise. Avec les mises à jour automatiques du navigateur Chrome, nous pouvons enfin respirer sur le plan de la sécurité."
>
> **Responsable de la sécurité, Blend**



Conclusion

Les navigateurs sont au cœur de la productivité des entreprises. Chaque jour, tout au long de la journée, les équipes modernes en dépendent pour travailler plus intelligemment et plus efficacement sur le Web depuis divers appareils et plates-formes.

Les navigateurs ne sont pas pour autant qu'un moteur de productivité. Pour les professionnels de la sécurité informatique, ils devraient également être vus comme une première ligne essentielle pour protéger les points de terminaison. Les navigateurs sont le lieu de rencontre entre le Web, les utilisateurs et les applications sur les points de terminaison. Ils sont donc idéalement situés pour surveiller et guider les comportements des utilisateurs en temps réel ainsi que pour appliquer des règles de sécurité critiques.

Le navigateur Chrome peut jouer un rôle stratégique dans la tactique de défense avancée d'une entreprise. Les fonctionnalités telles que la navigation sécurisée et Alerte mot de passe avertissent les utilisateurs des dangers du Web et en cas de non-respect des règles de sécurité, puis les orientent vers des comportements plus sûrs. Les administrateurs peuvent définir et appliquer des règles au niveau des points de terminaison, en profitant d'options telles que les listes de blocage
et d'autorisation pour les URL ainsi que pour les applications et les extensions, l'installation d'office d'applications et d'extensions ou leur blocage en fonction des autorisations, l'application de l'authentification à deux facteurs et l'autorisation d'une utilisation contrôlée des anciens navigateurs. Avec le navigateur Chrome et la gestion cloud du navigateur Chrome, les administrateurs peuvent facilement recueillir des données sur les appareils et l'activité des utilisateurs, ainsi que gérer et appliquer des règles de manière cohérente sur différents appareils et systèmes d'exploitation.

> Si vous êtes un professionnel de la sécurité informatique, vous devriez voir les navigateurs comme une première ligne essentielle pour protéger les points de terminaison. Découvrez comment le navigateur Chrome peut renforcer la sécurité de votre entreprise tout en améliorant votre efficacité et votre productivité.