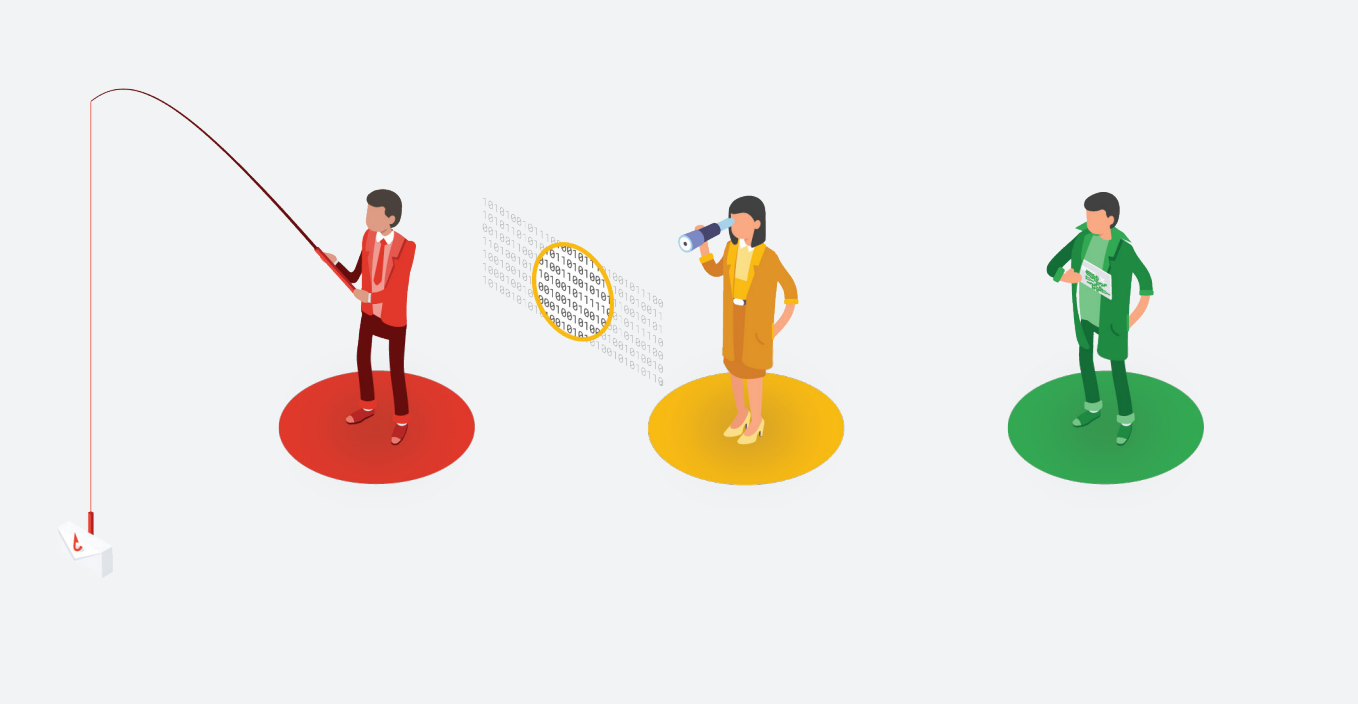
Sécurité cloud native pour les postes de travail

L'approche innovante de Chrome Enterprise pour protéger les données et simplifier la gestion informatique



chrome enterprise

chrome enterprise

Sommaire

Des problèmes auxquels il faut remédier

La sécurité des postes de travail n'est pas au point

La protection des postes de travail est l'un des plus grands défis des experts en opérations informatiques et en cybersécurité. Ils sont confrontés à des problèmes difficiles à résoudre et doivent lutter contre des attaques de plus en plus sophistiquées.

Les points de terminaison traditionnels sont complexes. Ils présentent généralement les caractéristiques suivantes :

1. Ils contiennent des centaines de logiciels que les personnes malintentionnées peuvent prendre pour cible, comme les versions obsolètes sans correctif et les packages logiciels non approuvés.
2. Ils sont vulnérables quand les utilisateurs consultent des sites Web malveillants, téléchargent des applications inconnues ou n'appliquent pas les mises à jour logicielles requises.
3. Ils contiennent plusieurs gigaoctets d'informations personnelles, de propriétés intellectuelles et d'identifiants de connexion.
4. Les frontières entre les processus sont insuffisantes, si bien qu'un pirate peut accéder à l'ensemble du système et du réseau d'entreprise à partir d'un seul module logiciel infecté.

Dans cet environnement, les experts en cybersécurité déploient des efforts considérables pour essayer de surveiller les postes de travail, d'identifier les vulnérabilités et de détecter les infections. Les responsables des opérations sont submergés de travail : ils s'efforcent d'imposer l'application d'images stables, de corriger et mettre à jour les micrologiciels, systèmes d'exploitation, utilitaires, pilotes, navigateurs et applications de centaines d'appareils distribués. Pour ne rien arranger, de plus en plus d'utilisateurs travaillent depuis leur domicile ou sur la route. Par conséquent, les outils et processus conçus pour les réseaux d'entreprise sont de moins en moins efficaces.

L’heure est venue de trouver un nouveau modèle

Vous avez aujourd’hui l’occasion de vous esortir de là et d’apporter des améliorations révolutionnaires à la sécurité et l’administration des postes de travail.

Les services informatiques peuvent commencer par exploiter les atouts naturels des architectures cloud en matière de sécurité et d’opérations. Surveiller les ressources d’information est plus simple quand elles sont stockées et partagées dans le cloud que sur des postes de travail vulnérables. Il est également bien plus simple de suivre et de mettre à jour des logiciels exécutés sur une plate-forme cloud centrale que sur des centaines d’appareils distants.

Ensuite, les fournisseurs informatiques ont entamé une refonte intégrale de la sécurité cloud native et proposent de nouvelles fonctionnalités exceptionnelles visant à renforcer la sécurité et simplifier la gestion des points de terminaison.

Dans ce livre blanc, nous expliquons comment Google a réinventé la sécurité des points de terminaison en tirant profit des avantages intrinsèques du cloud computing et en créant des défenses multicouches innovantes sur cinq niveaux : l’appareil, le micrologiciel, le système d’exploitation, le navigateur et l’application.

Les avantages suivants seront également étayés par plusieurs exemples :

1. Les fonctionnalités de sécurité innovantes de Google protègent les postes de travail de menaces spécifiques, telles que les logiciels malveillants, l’hameçonnage, les téléchargements furtifs et les menaces persistantes avancées.
2. Chrome Enterprise simplifie énormément les tâches opérationnelles, telles que la mise à jour des logiciels, la gestion des appareils perdus ou volés, ainsi que des règles de sécurité pour les appareils distribués.
3. Vous pouvez utiliser Microsoft Active Directory et les plus grands outils de gestion de la mobilité en entreprise (EMM) pour automatiser la gestion des points de terminaison.

Tirer profit des atouts naturels du cloud computing

Moins de ressources sur les postes de travail

L'un des avantages intrinsèques des architectures cloud est que la plupart des ressources d'information sont stockées dans le cloud et non sur les points de terminaison. Vous n'avez donc plus à craindre que votre base client, vos business plans, vos rapports sur les revenus, les données concernant vos employés ou vos programmes logiciels soient compromis en cas de perte ou de vol d'un ordinateur portable. Quand la sécurité d'un appareil est compromise, les personnes malintentionnées ont beaucoup moins de chance d'y trouver des numéros de carte de crédit, des informations médicales sur vos employés ou des mots de passe qui leur donnent accès aux systèmes financiers de l'entreprise.

Une fenêtre d'attaque réduite

Dans une infrastructure cloud, le nombre de logiciels installés sur les postes de travail est très limité. Les appareils distribués ont toujours besoin d'un micrologiciel et d'un système d'exploitation, mais les dizaines d'utilitaires, de pilotes, de navigateurs, d'applications professionnelles et personnelles qui s'accumulent généralement sur les points de terminaison traditionnels deviennent superflus. Ces architectures présentent bien moins de failles exploitables que les infrastructures traditionnelles, et nécessitent très peu de composants logiciels à installer, gérer et protéger.

Des mises à jour rapides et fréquentes

Avec les points de terminaison traditionnels, il faut sans cesse appliquer des correctifs et des mises à jour aux composants logiciels des appareils à travers le pays ou le monde. En outre, dès qu'une nouvelle faille est annoncée ou qu'un nouveau type d'attaque est découvert, les experts en cybersécurité et en opérations doivent réagir instantanément, et trouver rapidement des correctifs et contrôles supplémentaires pour des centaines de points de terminaison. Plus la "porte" reste ouverte, plus la probabilité que des pirates hostiles saisissent cette occasion augmente.

Les architectures cloud permettent de centraliser le déploiement et la gestion des contrôles, ainsi que la mise à jour des logiciels. L'actualisation des postes de travail demande donc beaucoup moins d'efforts.

Appareil : sécurité intégrée et cohérence

Les architectures cloud sont un terrain propice à l'innovation en matière de sécurité et de gestion. Pour illustrer notre propos, intéressons-nous tout d'abord aux appareils Chrome, tels que les ordinateurs portables et tablettes équipés de Chrome OS et du navigateur Chrome. De nombreux fabricants réputés proposent désormais des Chromebooks, y compris Acer, ASUS, Dell, Google, HP, Lenovo et Samsung.

Le module matériel de sécurité

Tous les Chromebooks récents sont équipés d'un module matériel de sécurité conçu selon les spécifications indiquées par Google. Ce module regroupe une mémoire flash, des mémoires ROM et RAM, ainsi que des fonctionnalités de détection des accès non autorisés sur une puce dédiée, afin de décourager toute tentative de piratage des informations stockées sur le module. Les données sensibles et les clés de chiffrement sont stockées sur le module matériel de sécurité afin de les rendre inaccessibles au système d'exploitation, et de les protéger contre certains types d'attaques par canaux cachés entraînant des fuites d'informations et d'attaques physiques d'injection de fautes.

Chiffrement et séparation des données utilisateur

Tous les Chromebooks chiffrent les données et les paramètres utilisateur par défaut. Ce chiffrement ne peut pas être désactivé par les utilisateurs (ou quiconque).

En outre, les paramètres et données utilisateur sont tous associés à une clé de chiffrement unique. Dans la grosse majorité des cas, pour utiliser cette clé, un pirate devrait à la fois connaître le mot de passe de l'utilisateur et avoir accès au module de sécurité. Les individus malveillants auront donc beaucoup de mal à lire les données des utilisateurs : même s'ils possèdent un Chromebook et le code secret d'un utilisateur, ils ne peuvent pas déchiffrer et lire ses données.

L'isolation des données utilisateur présente un autre avantage : le partage d'appareils avec des collègues ou des proches comporte moins de risques, tout comme des pratiques novatrices telles que le "Grab and Go" pour les appareils de prêt et les intérimaires.

Scénario : empêcher une violation d'initié

Xavier, Yao et Zelda sont trois prestataires qui travaillent à tour de rôle sur un même Chromebook en fonction des jours. Il s'avère que Xavier est un pirate amateur et souhaite s'attaquer à un serveur géré par Zelda. Il sait que des algorithmes et des logiciels propriétaires inestimables sont stockés sur ce serveur. Xavier se connecte au Chromebook et peut l'utiliser pour réaliser ses propres tâches, mais il ne parvient pas à accéder aux identifiants de Zelda, ni à ses connexions réseau, données ou autres paramètres. Les données de ce serveur sont en sécurité.

Cohérence sur tous les points de terminaison

Les fabricants de Chromebooks ont tous convenu de respecter les spécifications de Google en matière de qualité, de performances et de sécurité, ou de proposer des caractéristiques supérieures. Google vérifie et approuve le design des appareils avant qu'ils soient commercialisés sous la marque Chrome. Les fabricants se sont également engagés à utiliser la même version du micrologiciel, du système d'exploitation Chrome et du navigateur Chrome que sur les autres Chromebook (Figure 1).

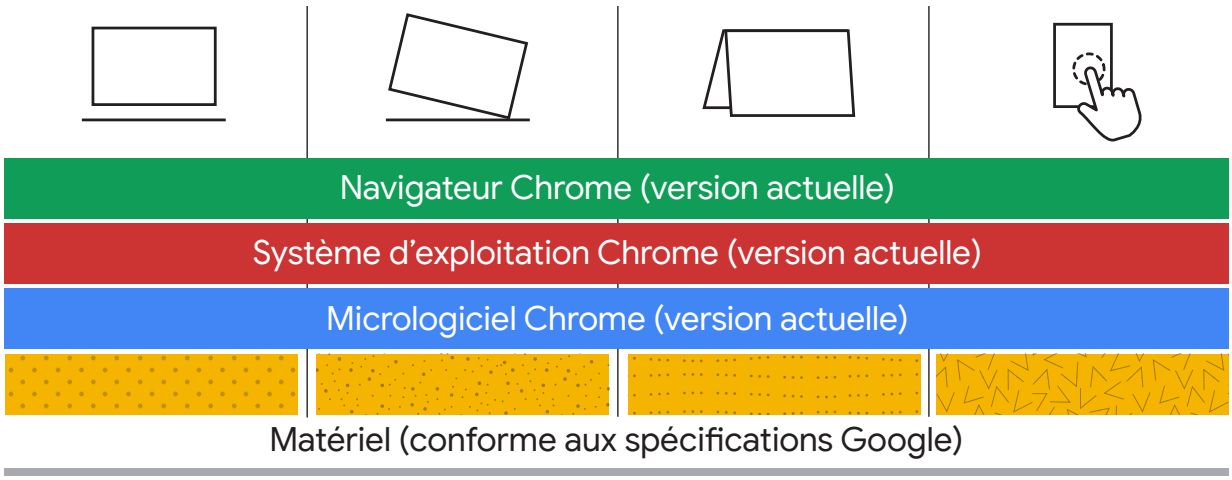


Figure 1 : pour unifier l'expérience utilisateur et simplifier la gestion informatique, tous les Chromebooks exécutent la même version du micrologiciel, du système d'exploitation Chrome et du navigateur Chrome.

Ce point commun est un grand avantage pour les utilisateurs, comme pour les administrateurs. Les utilisateurs bénéficient d'une expérience cohérente et d'un plus grand niveau de confort sur tous les Chromebooks. Les experts en sécurité et en opérations peuvent proposer un environnement standard. Ils n'ont plus à gérer plusieurs versions du micrologiciel, ou plusieurs systèmes d'exploitation, utilitaires et navigateurs, ni à redouter que des versions logicielles incompatibles ne créent des failles de sécurité. En cas de problème, la résolution est bien plus simple et rapide.

Des choix avisés en matière de sécurité

Google travaille en collaboration avec les partenaires de son réseau pour identifier les fonctionnalités et les paramètres par défaut qui contribuent à renforcer la sécurité des utilisateurs qui ne s'y connaissent pas en la matière, ni en informatique d'ailleurs. Par exemple, nous avons indiqué un peu plus tôt que toutes les données utilisateur sont chiffrées par défaut. Nous illustrerons cette fonctionnalité plus loin dans ce document.

Micrologiciel : une chaîne de vérification

Si nous devions choisir un adjectif pour caractériser les attaques ciblées les plus sophistiquées, ce serait la “persistance”. Dans ce genre d’attaques, les pirates implantent généralement un code ou des scripts sur les points de terminaison afin de maintenir leur présence sur les postes de travail après un redémarrage ou une panne système.

Les architectures cloud contrent un grand nombre d’attaques courantes utilisées par les pirates pour assurer leur persistance sur les points de terminaison traditionnels. Par exemple, si les utilisateurs ne peuvent pas installer de pilotes ou de scripts sur les points de terminaison, ces derniers ne peuvent pas être utilisés pour stocker un code malveillant qui persisterait après un redémarrage.

Cependant, les personnes malintentionnées peuvent toujours essayer d’injecter un code dans le micrologiciel accessible en écriture, le système d’exploitation et le navigateur qui sont stockés sur l’appareil.

Pour prévenir ce genre d’attaques, Google emploie une technique appelée le “démarrage validé” qui consiste à vérifier que le code exécuté pour le micrologiciel, le système d’exploitation et le navigateur après le redémarrage de l’appareil correspond parfaitement au code de Google.

Scénario : bloquer un programme malveillant furtif

Bela, une cybercriminelle, parvient à pirater un Chromebook et à obtenir les droits de super-utilisateur. Elle remonte directement la partition racine en lecture-écriture, puis ajoute un programme malveillant furtif sous la forme d’un module noyau. Cependant, au redémarrage suivant, la signature de cette partie de la partition racine ne correspond pas à la signature attendue. Le processus de démarrage est interrompu et l’appareil redémarre en utilisant l’image de back-up du micrologiciel et du système d’exploitation. Après le redémarrage, Bela ne peut plus utiliser le programme malveillant furtif pour contrôler l’appareil.

Au démarrage, le micrologiciel accessible en lecture seule du Chromebook utilise une signature et un hachage signé afin de vérifier que le micrologiciel accessible en écriture correspond parfaitement à l'image validée par Google. Autrement dit, il produit un hachage pour le code du micrologiciel et vérifie qu'il correspond au hachage signé. Le micrologiciel accessible en écriture ainsi validé utilise le même procédé pour vérifier le noyau, qui à son tour va vérifier tous les blocs de code du système d'exploitation et du navigateur Chrome. La moindre différence ou suspicion d'un logiciel malveillant entraîne l'interruption immédiate du processus de démarrage. L'appareil redémarre à partir d'une version de sauvegarde du micrologiciel accessible en écriture et du système d'exploitation (Figure 2).

Le démarrage validé a le double avantage de protéger les appareils contre les attaques sérieuses et de dispenser le personnel des opérations de la tâche fastidieuse qui consiste à réparer les fichiers et micrologiciels infectés.

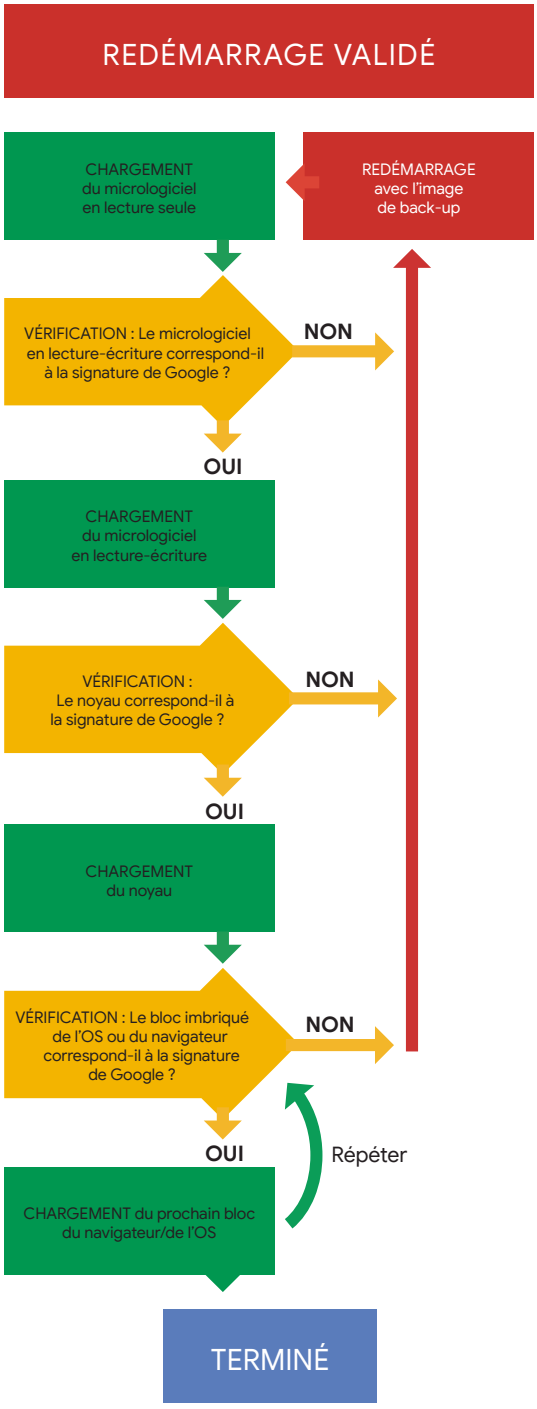


Figure 2 : le processus de démarrage validé garantit que le micrologiciel, le système d'exploitation et le navigateur n'ont pas été altérés.

Système d'exploitation : bac à sable des processus et mises à jour en arrière-plan

Le système d'exploitation Chrome offre de nombreuses fonctionnalités de sécurité qui protègent les applications et dispensent les équipes informatiques des fastidieuses mises à jour et applications de correctifs.

Séparation des droits et bac à sable des processus

Plusieurs types de cyberattaques utilisent des sites Web ou applications cloud infectés pour prendre contrôle des composants logiciels des points de terminaison.

Un environnement cloud natif comprend bien moins de composants du système d'exploitation, d'utilitaires, de pilotes et d'autres composants logiciel susceptibles d'être infectés. L'architecture de Chrome OS va encore plus loin pour empêcher que des applications contrôlées par des pirates puissent infecter d'autres logiciels.

Chrome OS isole notamment les processus dans des bacs à sable. Ils constituent des frontières nettes entre les processus en cours d'exécution, qui empêchent les applications de communiquer entre elles, sauf dans des cas très précis. Les droits de chaque processus en cours d'exécution sont strictement limités au minimum nécessaire. À l'instar des entreprises qui limitent l'accès aux informations aux seules personnes ayant besoin de les connaître pour des raisons de sécurité, Chrome OS limite les interactions entre les processus aux seules nécessaires.

Scénario : rejeter les rançongiciels

Arjun prend une pause et consacre quelques minutes à la recherche d'un nouveau fond d'écran pour son Chromebook. Malheureusement, le site Web consacré aux fans de Fortnite sur lequel il atterrit est un piège contrôlé par des cybercriminels. Quand il clique sur le lien de téléchargement du fichier, un code malveillant tente de chiffrer l'ensemble des fichiers et données stockés sur le Chromebook. Heureusement, les actions du code sont contenues dans un seul bac à sable de processus. Le message "Vous ne pouvez pas exécuter ce fichier" apparaît à l'écran et le rançongiciel est intercepté avant d'accéder aux données utilisateur.

Mises à jour du système d'exploitation en arrière-plan

La tâche la plus complexe pour les équipes chargées de la sécurité et des opérations est généralement l'actualisation des systèmes d'exploitation. Sur les postes de travail traditionnels, les mises à jour du système d'exploitation sont une source d'irritation pour les utilisateurs finaux. Les postes de travail étant inutilisables pendant les mises à jour, les utilisateurs sont bloqués pour une durée déterminée, qui peut s'étendre de quelques minutes à plus d'une heure. Cela se traduit concrètement par une baisse de la productivité, voire par des pensées négatives envers le service informatique.

Pire encore, les utilisateurs refusent parfois d'appliquer les mises à jour, laissant leurs appareils à la merci de diverses attaques.

Google propose une solution innovante pour résoudre ce problème. Chaque appareil est équipé de deux versions du système d'exploitation, la version actuelle et la version précédente. Ainsi, pendant que l'appareil utilise le système d'exploitation actuel, une version plus récente peut être téléchargée et stockée en parallèle, en arrière-plan, sans même que l'utilisateur ne le remarque. Au prochain redémarrage, la nouvelle version du système d'exploitation est chargée en quelques secondes (Figure 3).

Cette méthode simplifie également le processus de démarrage validé dont nous avons parlé précédemment. Si au cours du démarrage, l'appareil détecte que le code du système d'exploitation en cours d'exécution a été altéré, il peut basculer instantanément sur la version précédente qui est certifiée sûre et déjà disponible sur l'appareil.

Les Chromebooks simplifient les mises à jour des composants du système d'exploitation. Pourtant, Google réalise une mise à jour de Chrome OS environ toutes les six semaines, soit bien plus souvent que les autres grands systèmes d'exploitation. De plus, Google réagit très rapidement aux annonces de nouvelles failles de sécurité en déployant des correctifs de sécurité le plus tôt possible pour réduire la fenêtre d'exposition.

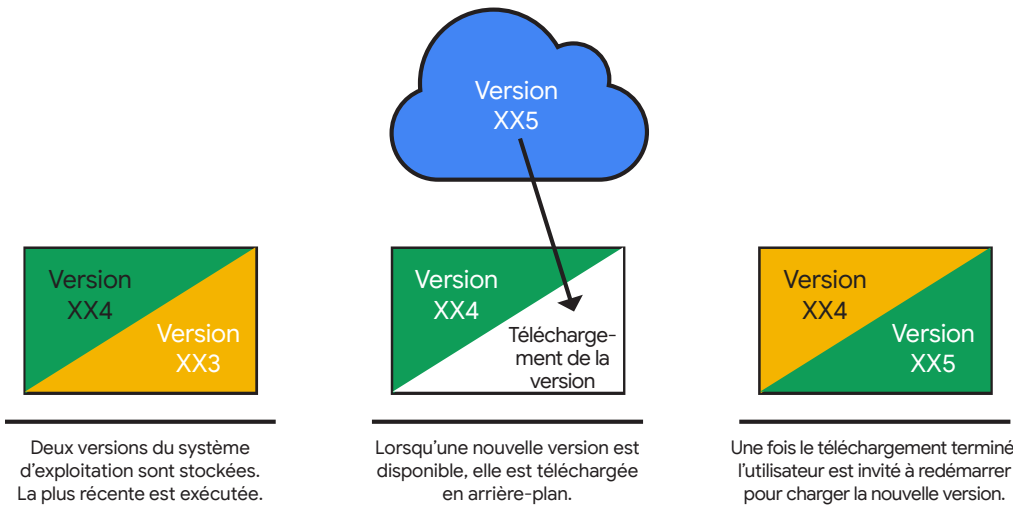


Figure 3 : les nouvelles versions du système d'exploitation sont téléchargées en arrière-plan, sans interrompre le travail des utilisateurs.

Navigateur : isolation de sites, navigation sécurisée et authentification à deux facteurs

Sur les Chromebooks, toutes les interactions avec le Web se déroulent dans le navigateur Chrome. Les utilisateurs bénéficient ainsi des fonctionnalités de sécurité innovantes du navigateur phare de Google.

Bac à sable des onglets et isolation de sites

Le concept de bac à sable qui s'applique dans Chrome OS est également utilisé dans le navigateur Chrome. Chaque onglet ouvert dans le navigateur est isolé dans son propre bac à sable, ce qui limite grandement la propagation des attaques d'un onglet à l'autre.

Le principe peut même être étendu aux sites Web. Souvent, un même onglet est utilisé pour accéder à plusieurs sites Web. Par exemple, la page d'un site Web en HTML peut contenir des images, des vidéos et un script provenant chacun d'un autre site. L'isolation de sites permet de séparer les processus de chacun de ces sites (Figure 4). Dans le navigateur Chrome, les administrateurs peuvent isoler tous les sites ou les sites de leur choix.

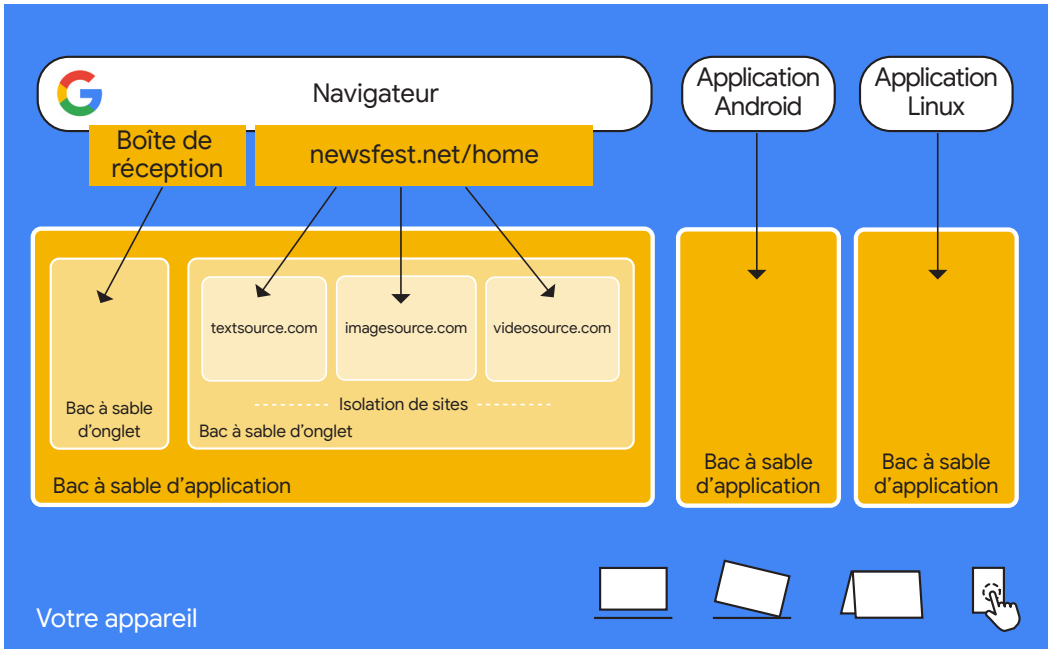


Figure 4 : Chrome OS et le navigateur Chrome offrent plusieurs niveaux d'isolation (sites, onglets et applications).

Ces fonctionnalités protègent les systèmes de certaines menaces, comme les scripts intersites universels (UXSS) et les attaques d'exécution spéculative par canaux cachés (telles que Spectre et Meltdown). Ces attaques reposent sur un site Web malveillant, qui tente d'accéder aux processus ou aux données en mémoire appartenant à un autre site Web.

Navigation sécurisée

Parmi les plus grandes menaces qui pèsent actuellement sur les entreprises, les logiciels malveillants et les tentatives d'hameçonnage émanant de sites Web infectés sont les plus courantes.

La fonctionnalité de navigation sécurisée Google avertit l'utilisateur quand il tente d'accéder à un site Web qui contient un logiciel malveillant ou des éléments d'hameçonnage, ou quand il tente de télécharger des fichiers suspects. Elle repose sur un service Google qui analyse quotidiennement des milliers de sites Web dangereux et protège trois milliards d'appareils.

Les messages de la navigation sécurisée sont affichés dans les fenêtres du navigateur Chrome, mais aussi dans les recherches Google et les applications Android pour informer l'utilisateur de la dangerosité des sites Web, et dans les messages Gmail pour prévenir l'utilisateur que les liens qu'ils contiennent renvoient vers des sites malveillants.

Scénario : esquiver une tentative d'hameçonnage

Emily est directrice financière d'une petite entreprise de fabrication. Elle reçoit un e-mail du PDG, dans lequel il indique vouloir virer immédiatement 20 000 $ à un nouveau fournisseur en Chine, pour commander un composant bientôt en rupture de stock. Emily sait que le PDG se déplace souvent en Chine pour négocier avec les fournisseurs, donc l'e-mail lui semble légitime. Pourtant, quand elle clique sur le lien contenu dans l'e-mail, censé la diriger vers le site Web du nouveau fournisseur, elle reçoit un avertissement la prévenant que le site est frauduleux et l'invitant à cliquer sur le lien "Retour à la sécurité" de la fenêtre. Grâce à la navigation sécurisée, Emily a esquivé une tentative d'hameçonnage visant à compromettre les messageries professionnelles.

Clés de sécurité et authentification à deux facteurs

L'authentification à deux facteurs (également appelée "validation en deux étapes") est une protection supplémentaire des systèmes et des données, même en cas de piratage des identifiants de l'utilisateur. Elle nécessite que les utilisateurs fournissent quelque chose qu'ils connaissent, comme un mot de passe, ainsi que quelque chose qu'ils possèdent, comme une clé d'authentification ou un code envoyé sur leur smartphone.

Google propose un moyen simple et rapide, voire le plus simple et le plus rapide au monde, de mettre en place une authentification à deux facteurs efficace. Les utilisateurs n'ont qu'à se rendre dans leur compte Google, sélectionner "Validation en deux étapes" et choisir leur seconde méthode d'authentification. Ils ont le choix entre saisir un code envoyé par SMS, appuyer sur une notification sur leur téléphone ou insérer une clé de sécurité Titan dans l'un des ports USB de leur Chromebook. Pour plus de facilité, les utilisateurs peuvent désigner des appareils vérifiés et se connecter à partir de ces appareils sans recourir à la seconde méthode d'authentification.

Applications : détection des logiciels malveillants, liste blanche et liste noire

Les Chromebooks sont compatibles avec un large éventail d'applications, y compris les applications Android, les applications bureautiques de productivité telles que Gmail, Google Docs, Google Sheets, Google Slides et Google Drawings, les extensions Chrome, les applications Linux et les applications Web progressives (progressive web apps ou PWA : des applications qui offrent un chargement rapide et une réactivité similaire à celle des applications installées en local).

Quand les entreprises mettent à la disposition de leurs utilisateurs des applications développées par Google via le Chrome Web Store et des applications Android via le Google Play Store, elles bénéficient de fonctionnalités dont le but est de renforcer la sécurité et de simplifier l'administration.

Détection des logiciels malveillants côté serveur et désinstallation à distance

Google Play Protect est le service de protection contre les menaces mobiles le plus déployé dans le monde, qui compte deux milliards d'utilisateurs par jour. Toutes les applications Android présentes dans le Google Play Store ont fait l'objet de tests de sécurité rigoureux par nos experts en sécurité Android. Les applications et développeurs qui ne respectent pas les règles de Google ne sont pas acceptés dans le Play Store.

Ce n'est pas tout : Google Play Protect analyse et vérifie en permanence les applications cataloguées dans le Google Play Store. Quand il détecte un élément malveillant dans une application du Google Play Store, l'application concernée est immédiatement retirée du catalogue, mais aussi désinstallée de tous les systèmes sur lesquels elle était téléchargée.

Sélection et liste blanche d'applications via le Google Play Store

Trop souvent, les utilisateurs téléchargent des applications présentant des failles ou développées par des personnes malintentionnées cherchant à dérober des données, et leur facilitent ainsi la tâche.

Scénario : diminution des cas de "shadow IT"

Carlos est responsable d'une équipe marketing dont les membres sont répartis sur quatre continents. Il souhaite simplifier la planification et améliorer la communication au sein de l'équipe à l'aide d'un outil collaboratif. Il s'intéresse à un article intitulé "Les 20 meilleurs outils collaboratifs en ligne", sans se douter que la plupart des applications citées ne proposent pas de fonctionnalités de gestion et de sécurité professionnelles. Heureusement, avant d'avoir testé une seule des applications de l'article, il pense à consulter la plate-forme Google Play d'entreprise de son organisation. Il y trouve deux applications de collaboration approuvées, Slack et Google Hangouts. Elles offrent chacune des fonctionnalités et un niveau de sécurité exceptionnels. Elles ont également l'avantage d'être couvertes par le service informatique de l'entreprise. En utilisant l'une de ces applications, l'équipe de Carlos pourra interagir avec tous les autres employés de l'entreprise les ayant également adoptées.

Depuis des dizaines d'années, les administrateurs informatiques tentent d'enrayer les téléchargements risqués soit en incitant les utilisateurs à installer uniquement des applications approuvées, soit en verrouillant les postes de travail, de sorte que seules les applications approuvées puissent être exécutées. La première approche ne s'est pas révélée efficace, puisque la liste des applications approuvées est inévitablement trop restreinte pour satisfaire les besoins de tous les utilisateurs, qui recherchent autant des applications professionnelles pour travailler, que des applications personnelles pour se divertir. La seconde approche n'a pas eu plus de succès, d'une part parce que les technologies permettant de verrouiller les postes de travail sont compliquées à mettre en place, et d'autre part, car les utilisateurs y sont fortement réfractaires.

Grâce aux technologies Web, les experts en sécurité et en opérations disposent de moyens efficaces pour tarir le flux d'applications non approuvées sans décevoir ou agacer les utilisateurs.

Le Google Play Store contient des milliers d'applications professionnelles de productivité, de communication, de collaboration et de gestion des processus métier, ainsi que des applications d'actualités, de divertissement et de jeux vidéo. Toutes ces applications sont préalablement testées par l'équipe chargée de la sécurité Android pour vérifier l'absence de toute faille ou autre problème de sécurité.

Les administrateurs peuvent créer une plate-forme Google Play d'entreprise propre à leur organisation et sélectionner un ensemble varié et conséquent d'applications. Ils peuvent, par exemple, proposer aux employés de leur entreprise un grand nombre d'applications de productivité et de collaboration, et limiter le nombre de jeux vidéo et d'applications de réseaux sociaux (Figure 5).

S'ils estiment que cela est nécessaire, ils peuvent même aller plus loin et intégrer une liste blanche d'applications dans la plate-forme Google Play d'entreprise, afin que tous les membres de l'organisation utilisent les mêmes outils de productivité et de collaboration, et disposent d'un choix limité pour les autres types d'applications.

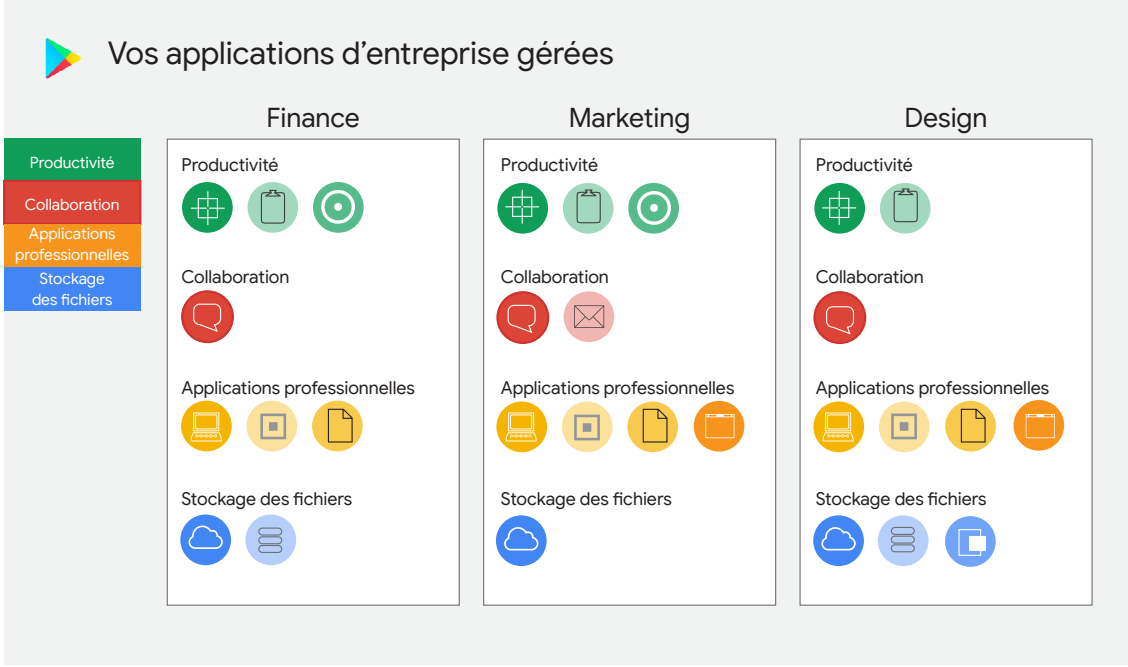


Figure 5 : avec une plate-forme Google Play d'entreprise, chaque service de l'entreprise peut accéder à une liste d'applications sélectionnées et approuvées.

Administration centralisée avec Chrome Enterprise

Grâce à Chrome Enterprise, les équipes chargées de la sécurité et des opérations peuvent gérer de manière centralisée les règles appliquées aux Chromebooks et autres postes de travail équipés de Chrome OS, ainsi que les règles appliquées aux navigateurs Chrome sur les systèmes Windows, Mac et Linux. La licence Chrome Enterprise regroupe des fonctionnalités de gestion des appareils et une assistance 24h/24, 7j/7 de Google, afin d'aider les entreprises à évoluer vers des environnements comprenant des dizaines de milliers d'utilisateurs et d'appareils.

Présentation des quelques règles Chrome Enterprise

Chrome Enterprise permet aux administrateurs de définir et d'appliquer plus de 300 règles de configuration et de sécurité sur les points de terminaison. Voici quelques-unes des fonctionnalités de sécurité pour les appareils Chrome gérés :

Activation et annulation de la gestion des appareils. Les administrateurs peuvent inscrire des appareils ou autoriser les utilisateurs à inscrire des appareils, afin qu'ils soient gérés et protégés par les règles Chrome Enterprise définies pour l'entreprise de l'utilisateur. Les administrateurs ont la possibilité d'annuler la gestion des appareils pour désactiver les règles sur les appareils et leur interdire l'accès aux ressources d'entreprise.

Désactivation des appareils à distance. En cas de vol ou de perte d'un appareil, il est possible de le désactiver à distance.

Restriction des connexions. Les administrateurs peuvent autoriser les connexions anonymes (navigation en tant qu'invité), exiger un compte Google ou G Suite, ou autoriser l'accès à seulement certains utilisateurs.

Configuration du mode Éphémère (effacement des données utilisateur à la déconnexion). Les administrateurs peuvent configurer les appareils en mode Éphémère afin que les données et les paramètres des utilisateurs (y compris l'historique du navigateur, les extensions et données d'extensions, et les données Web comme les cookies) soient effacés lors de leur déconnexion. Le mode Éphémère est idéal pour renforcer la sécurité des appareils partagés, des kiosques et des utilisateurs temporaires.

Interdiction ou obligation d'installer des applications Web et extensions de navigateur. Les administrateurs peuvent interdire complètement l'installation d'applications Web Chrome et d'extensions de navigateur (petits programmes logiciels permettant de personnaliser le navigateur), interdire l'installation d'applications et extensions spécifiques, ou contraindre les utilisateurs à installer des applications et extensions uniquement à partir d'URL spécifiques. Ils peuvent également forcer l'installation d'applications et extensions spécifiques.

Blocage d'applications en fonction d'autorisations. De nombreuses applications Chrome et extensions de navigateur demandent des autorisations pour utiliser les ressources de l'appareil sur lesquels elles sont installées. Les administrateurs peuvent bloquer l'installation des applications et extensions qui demandent des autorisations spécifiques, telles que : la capture du contenu de l'écran, d'une fenêtre ou d'un onglet, la lecture du contenu du presse-papiers, l'enregistrement du son ou de l'image avec le micro ou l'appareil photo, la géolocalisation de l'utilisateur, la recherche des métadonnées

du réseau de l'appareil ou le contournement des fonctionnalités de gestion de l'alimentation de l'appareil. Grâce à cette règle, le service informatique limite les risques tout en offrant aux utilisateurs la liberté d'installer des applications "inoffensives", qui ne menacent pas la sécurité de l'appareil.

Désactivation du Bluetooth et de la géolocalisation. Le Bluetooth et la localisation peuvent être désactivés sur l'appareil.

Restriction de l'utilisation des périphériques de stockage externes. L'utilisation de périphériques de stockage externes, tels que les clés USB, les disques durs externes, stockages optiques, cartes SD et autres cartes mémoire, peut être complètement interdite ou autorisée uniquement en mode lecture seule.

Gestion de l'accès à distance et de l'authentification unique. Les administrateurs peuvent configurer les paramètres de l'accès à distance et de l'authentification unique SAML, afin que les utilisateurs puissent accéder facilement au réseau et aux applications Web sans compromettre la sécurité.

Suivi des appareils et des utilisateurs. Pour chaque appareil, les administrateurs peuvent créer des rapports pour contenant des informations telles que : les niveaux du système d'exploitation et du micrologiciel, les statistiques d'utilisation du processeur et de la mémoire vive, les périphériques de stockage connectés, les statistiques générales d'utilisation, les données de diagnostic, la liste des utilisateurs connectés récemment et la liste des utilisateurs actifs.

Administration déléguée et gestion souple

Chrome Enterprise permet de déléguer des tâches d'administration pour répartir la charge de travail et la responsabilité de la gestion des groupes et services aux personnes appropriées. Il est possible de créer des rôles pour accorder aux administrateurs des autorisations différentes pour consulter ou modifier les paramètres des applications, utilisateurs et appareils gérés.

Avec Chrome Enterprise, les administrateurs peuvent créer et appliquer les règles comme ils le souhaitent. Les règles peuvent concerner les utilisateurs et groupes d'utilisateurs, auquel cas chaque utilisateur est soumis aux mêmes règles sur tous ses appareils. À l'inverse, les règles peuvent concerner les appareils, auquel cas les règles seront appliquées sur tous les appareils, peu importe qui les utilisent.

Scénario : cette réunion doit rester privée

Votre PDG et votre directeur financier partent en déplacement à l'étranger pour négocier un accord très important. Si l'autre partie ou les services de renseignement du pays de destination venaient à surprendre les conversations qu'ils ont entretenues lors de leurs réunions stratégiques, votre entreprise s'exposerait à de grosses pertes. Heureusement, vous pouvez désactiver temporairement le Bluetooth, et bloquer les applications Web Chrome et extensions de navigateur qui peuvent accéder au microphone et à l'appareil photo de leur Chromebook. (Pensez à leur demander de redémarrer leur ordinateur pour que les modifications prennent effet.)

Optimisation de votre infrastructure de gestion

Chrome Enterprise dispose de sa propre console d'administration, mais peut tout aussi bien s'intégrer dans votre infrastructure de gestion existante.

Intégration dans Active Directory et Google Cloud Identity

La console d'administration de Chrome Enterprise s'intègre parfaitement dans Microsoft Active Directory et Google Cloud Identity. Cela signifie que vous pouvez inscrire des appareils Chrome dans Active Directory. Vous pouvez également transmettre les règles de Chrome aux utilisateurs et aux appareils appartenant aux groupes d'utilisateurs définis dans Active Directory.

Collaboration avec les meilleures solutions EMM

Les solutions de gestion de la mobilité en entreprise (EMM) aident les entreprises à inscrire, gérer et dépanner les ordinateurs portables, tablettes, smartphones et autres appareils mobiles. Si votre entreprise a investi dans des solutions EMM telles que Cisco Meraki, Citrix XenMobile, IBM MaaS360, ManageEngine Mobile Device Manager Plus, et VMWare Airwatch, vous pouvez continuer à les utiliser pour gérer les Chromebooks avec le reste de vos postes de travail.

Résumé : Une sécurité et un contrôle des opérations révolutionnaires

Avec le cloud computing, les entreprises ont l'occasion de repenser l'infrastructure traditionnelle de leurs postes de travail. En adoptant une infrastructure native cloud, elles peuvent grandement renforcer la sécurité et simplifier la gestion de ces postes de travail.

Les appareils Chrome exploitent les avantages intrinsèques du cloud computing, comme le stockage limité de ressources sur les postes de travail, une surface d'attaque réduite et des mises à jour rapides et simples. En outre, cette approche laisse entrevoir des fonctionnalités innovantes de sécurité et de gestion, comme les fonctionnalités de sécurité intégrées au matériel et au micrologiciel, l'utilisation optimale du bac à sable et du chiffrement au niveau de l'utilisateur, la mise à jour en arrière-plan des systèmes d'exploitation, la navigation sécurisée, l'authentification à deux facteurs simple, la liste blanche d'applications, ainsi que la gestion simplifiée des règles de sécurité et des opérations, facilement transposable pour des milliers d'utilisateurs et d'appareils.

Vous obtenez ainsi un environnement informatique qui combine les caractéristiques suivantes :

1. Conception sécurisée
2. Administration bien plus simple que celle des postes de travail traditionnels
3. Intégration directe dans l'infrastructure existante

En savoir plus sur la sécurité de Chrome Enterprise

(à l'adresse https://cloud.google.com/chrome-enterprise/security/)