chrome enterprise

Mettez votre entreprise à l'abri dans le cloud

Pour améliorer leur sécurité, les organisations investissent massivement dans des produits qui se targuent de les protéger des pirates, des espions et des failles. Malgré leurs efforts, le nombre de violations ne cessent d'augmenter.

> En 2019, le marché de la sécurité des données devrait **croître de 8,7 % pour atteindre 124 milliards de dollars**[1].

> En parallèle, aux États-Unis, le nombre de violations ciblées de grande ampleur **augmente chaque année de plus de 27 %**[2].

Bien que ces menaces soient toujours plus nombreuses et sophistiquées, les types d'attaques sont bien connus : il s'agit le plus souvent de logiciels malveillants, de rançongiciels et d'hameçonnage. Il n'est bien sûr plus question d'appliquer nos principes de sécurité habituels, aujourd'hui inefficaces. Nous devons trouver une solution nouvelle à un vieux problème.

Adoptez une approche unique pour sécuriser les points de terminaison avec Chrome Enterprise

Sécurité multicouche des appareils

Les couches d'un Chromebook sont interconnectées afin d'offrir des avantages uniques en matière de sécurité.

- Chiffrement des données utilisateur
- Protection contre l'altération du système d'exploitation
- Réduction de l'encombrement des données sur l'appareil
- Correctifs et mises à jour réguliers
- Prévention contre la négligence des utilisateurs

Applications gérées et isolées

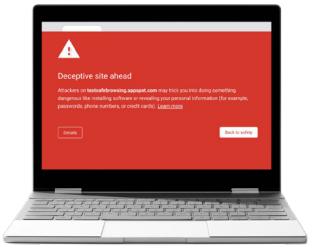
Les applications dangereuses restent hors de portée des utilisateurs.

- Limitation de la surface d'attaque grâce au bac à sable
- Application de règles d'accès
- Sécurisation de plusieurs écosystèmes, y compris le Chrome Web Store, Google Play, le Web et les applications Linux natives

[1] Ponemon and Accenture, 2017; [2] Gartner, 2018

chrome enterprise

Protégez votre entreprise des menaces bien connues avec Chrome Enterprise et la puissance de Google Cloud



Hameçonnage

Avec la navigation sécurisée Google, les utilisateurs sont avertis qu'ils ont affaire à un site malveillant avant d'y accéder.

Les clés de sécurité et la validation en deux étapes empêchent les pirates d'utiliser des mots de passe volés.

En cas d'attaque : La règle Alerte mot de passe exige que les utilisateurs modifient leur mot de passe lorsqu'ils l'utilisent sur un site non autorisé.

Rançongiciel

Le faible encombrement des données sur l'appareil limite la quantité de données pouvant faire l'objet d'une demande de rançon.

L'OS en lecture seule empêche l'exécution des fichiers en local.

En cas d'attaque : La fonctionnalité de démarrage validé vérifie au moment du démarrage que le système n'a pas été modifié.

Applications malveillantes

Les listes noires basées sur les autorisations contrôlent les extensions auxquelles l'utilisateur a accès.

La fonctionnalité **Google Play géré** simplifie l'organisation en groupe d'utilisateurs et la configuration des règles par application.

En cas d'attaque : Le bac à sable limite la surface d'attaque.

Pourquoi les Chromebooks ne nécessitent pas d'antivirus

Grâce à la lecture seule, les applications et extensions installées ne peuvent pas modifier le système d'exploitation.

Le bac à sable isole toute attaque sur une surface limitée.

Le démarrage validé empêche le démarrage d'un appareil compromis.

Un processus de vérification est requis pour toutes les extensions et applications.

Pourquoi les mises à jour Chromebook sont très efficaces

Aucun temps d'arrêt, les mises à jour s'effectuent en arrière-plan pendant que les utilisateurs travaillent.

L'utilisation de **deux versions de système d'exploitation** sur un appareil permet de travailler sur l'une pendant que l'autre est mise à jour.

La mise à jour s'applique au redémarrage en quelques secondes.

En savoir plus sur la sécurité de Chrome Enterprise :
cloud.google.com/chrome-enterprise/security