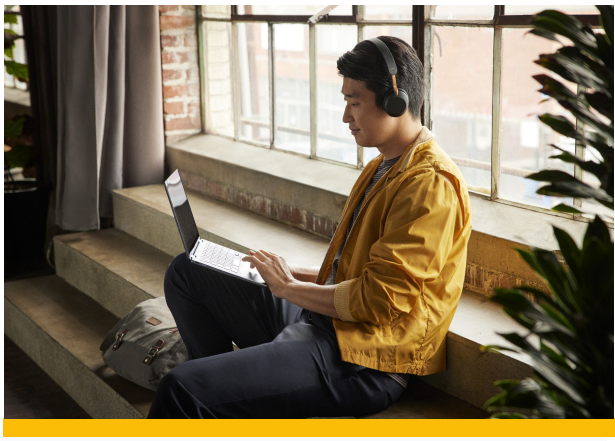
chromeOS

Sécurisez votre parc d'appareils avec ChromeOS

Les entreprises font face à des niveaux jamais atteints de propriété intellectuelle, de données et d'identités qui ne sont pas protégées par le pare-feu. Chaque point de terminaison est une porte d'entrée dans l'entreprise. La menace vient aussi de l'intérieur, l'erreur humaine étant un risque constant.

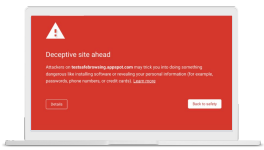
Protégez vos appareils grâce à ChromeOS et ses mesures de sécurité intelligentes intégrées, ses contrôles précis des règles et ses mises à jour automatiques qui offrent une protection ininterrompue. Protégez les utilisateurs et les données contre les rançongiciels, les logiciels malveillants et l'hameçonnage grâce à un OS en lecture seule et à des appareils chiffrés. Chaque niveau de la pile ChromeOS, qui est intégrée verticalement, renforce la sécurité, tandis que les mises à jour automatiques à l'échelle du système permettent de pérenniser votre protection.



En 2020, le marché mondial de la cybersécurité était **évalué à 167 milliards de dollars**[1].

En 2020, les violations de données ont exposé **plus de 36 milliards de dossiers**[2].

Protégez votre entreprise contre l'hameçonnage, les rançongiciels et les logiciels malveillants avec ChromeOS



Hameçonnage

La navigation sécurisée Google alerte les utilisateurs sur le point d'accéder à un site malveillant.

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

En cas d'attaque, la règle Alerte mot de passe oblige les utilisateurs à changer leur mot de passe s'ils s'en servent sur un site non autorisé.

Rançongiciels

Étant donné la faible quantité de données stockées sur les appareils, les données pouvant faire l'objet d'une demande de rançon sont limitées.

Les fichiers de l'OS en lecture seule empêchent l'exécution de programmes et d'applications malveillantes en local.

En cas d'attaque, la fonctionnalité Démarrage validé vérifie au démarrage que le système n'a pas été altéré.

Logiciels malveillants

L'ajout sur liste de blocage en fonction des autorisations permet de contrôler le type d'extensions accessibles.

Le Google Play d'entreprise facilite la gestion par groupes d'utilisateurs et le paramétrage de règles pour chaque application.

En cas d'attaque, le système de bac à sable en limite la portée.

[1] Grand View Research, 2021 ; [2] RiskBased Security, 2020

chromeOS

Protection contre les rançongiciels, les logiciels malveillants et l'hameçonnage

Fichiers de l'OS en lecture seule : les fichiers système sont stockés sur une partition distincte pour garantir que les fichiers de l'OS ne puissent pas être modifiés par des applications ni des extensions. Les rançongiciels n'ont donc pas accès à ces fichiers.

Exécutables bloqués : les exécutables, qui sont susceptibles de contenir des éléments malveillants, ne peuvent pas être ouverts sur ChromeOS. Seules les applications issues du Google Play Store et dans lesquelles aucun logiciel malveillant n'a été détecté peuvent être exécutées sur ChromeOS.

Matériel chiffré : les appareils ChromeOS sont chiffrés par défaut à l'aide d'une clé unique, ce qui rend la lecture des données utilisateur particulièrement difficile pour les pirates informatiques. Ce chiffrement ne peut pas être désactivé.

Démarrage validé : la fonctionnalité Démarrage validé vérifie lors du redémarrage que le micrologiciel et le système d'exploitation n'ont pas été altérés ni corrompus. Si c'est le cas, une version précédente de l'OS est restaurée.

Système de bac à sable et isolation des sites : le système de bac à sable et l'isolation des sites limitent les menaces à une seule application ou à un seul onglet pour protéger le reste de l'OS.

Gestion centralisée et à distance

Règles de gestion : gérez et configurez vos appareils ChromeOS de façon centralisée avec plus de 500 règles, y compris des paramètres d'authentification.

Applications et extensions autorisées : empêchez les utilisateurs d'installer certaines applications et extensions en fonction des autorisations nécessaires à leur exécution. Empêchez les utilisateurs de télécharger des applications et des extensions malveillantes grâce au Chrome Web Store et au Google Play Store d'entreprise, et à Google Play Protect.

Mode Éphémère (effacement des données utilisateur lors de la déconnexion) : configurez les appareils de sorte que l'ensemble des données et des paramètres soient automatiquement effacés lorsque l'utilisateur se déconnecte.

Protection en cas de perte ou de vol (Powerwash et désactivation à distance) : désactivez ou effacez les appareils perdus ou volés à distance, et affichez un message indiquant à la personne l'ayant retrouvé où le restituer.

Gestion de l'accès distant et de l'authentification unique : définissez des paramètres pour l'accès distant et l'authentification unique (SSO) basée sur le protocole SAML, pour que les utilisateurs puissent accéder au réseau et aux applications Web en bénéficiant d'un juste équilibre entre confort et sécurité.

Rapports : les rapports permettent d'obtenir des informations telles que la dernière version du système d'exploitation et les dates d'expiration des mises à jour automatiques de votre parc d'appareils.

Mises à jour automatiques pour protéger votre parc

Mises à jour rapides, fréquentes et régulières : les mises à jour du micrologiciel et des fonctionnalités ChromeOS interviennent toutes les six semaines, soit beaucoup plus souvent que pour la majorité des autres systèmes. Les mises à jour sont appliquées lors du redémarrage et ne prennent que quelques secondes.

Coûts d'assistance inférieurs : les mises à jour régulières du système d'exploitation et l'application manuelle de correctifs, qui peuvent être coûteuses, ne sont plus nécessaires avec ChromeOS.

Aucun temps d'arrêt ni interruption : les mises à jour s'effectuent automatiquement en arrière-plan pendant que l'utilisateur travaille. Il y a deux versions de l'OS, ce qui signifie que l'une peut être utilisée pendant que l'autre est mise à jour. Ainsi, les données restent protégées et les employés peuvent continuer à travailler.

Pas de différences selon le fabricant : tous les appareils ChromeOS, quel que soit le fabricant, bénéficient des mêmes mises à jour.

→ En savoir plus sur la sécurité de ChromeOS : https://chromeenterprise.google/os/security