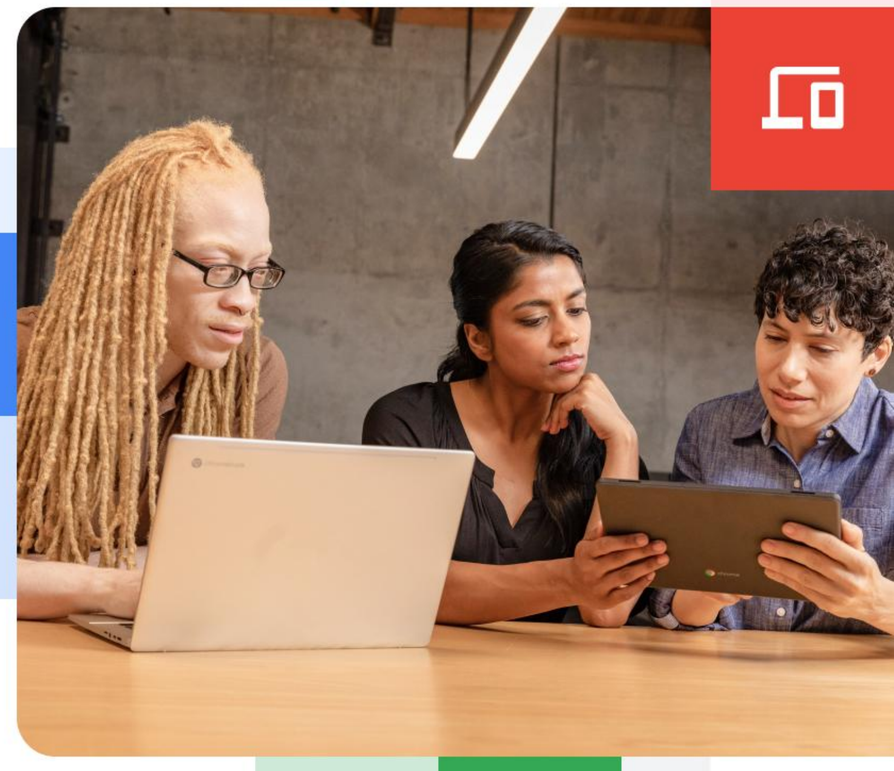
chromeOS

L'OS prêt à l'emploi le plus sûr qui soit.



Huit raisons qui placent ChromeOS devant ses concurrents

Selon un récent rapport d'analyse concurrentielle d'Atredis Partners, entreprise de recherche en sécurité, ChromeOS est sécurisé dès son premier démarrage.

Grâce à sa philosophie zéro confiance, ChromeOS n'approuve automatiquement aucun utilisateur ou appareil. Tout est systématiquement vérifié pour assurer une sécurité optimale, de vos tentatives de connexion aux fichiers que vous souhaitez télécharger. Examinons les huit points clés, confirmés par le rapport, qui démontrent que ChromeOS protège les utilisateurs, les données et les appareils, et ce, à tous les niveaux[1].

1 "Les appareils ChromeOS démarrent toujours de manière sécurisée"

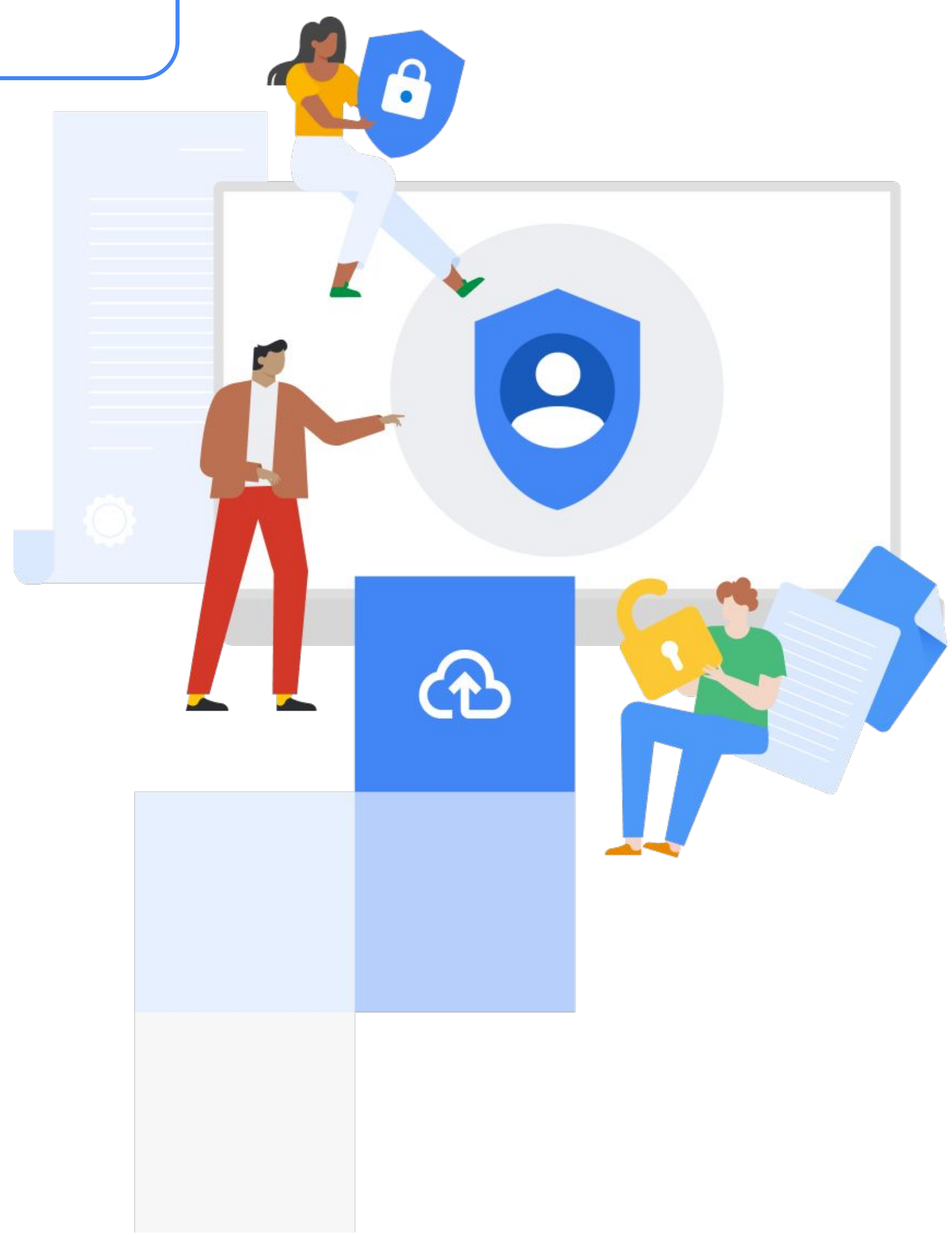
Aucune attaque réussie par virus ou rançongiciel n'a jamais été signalée sur ChromeOS[2].

ChromeOS vérifie systématiquement les changements apportés à son micrologiciel grâce au démarrage validé, une norme de sécurité par défaut supérieure à celle de macOS ou Windows 11. Si du code inconnu est détecté, ChromeOS revient automatiquement à une version antérieure pour protéger votre appareil[1].

chromeOS

2 "Les données utilisateur sont chiffrées par défaut"

ChromeOS est le seul système d'exploitation conçu pour empêcher par défaut qu'un utilisateur puisse accéder aux données d'autres utilisateurs.



L'intégralité des données stockées sur le disque dur est chiffrée à l'aide d'ensembles d'identifiants uniques à chaque utilisateur, et les données des utilisateurs invités sont immédiatement supprimées après déconnexion, faisant de ChromeOS le système d'exploitation idéal pour les appareils partagés. Les systèmes d'exploitation comme Windows 11 et macOS doivent être configurés spécifiquement pour prendre en charge le chiffrement, et les administrateurs peuvent toujours accéder aux données des autres utilisateurs[1].

3 "Il n'existe pas d'administrateur dans ChromeOS"

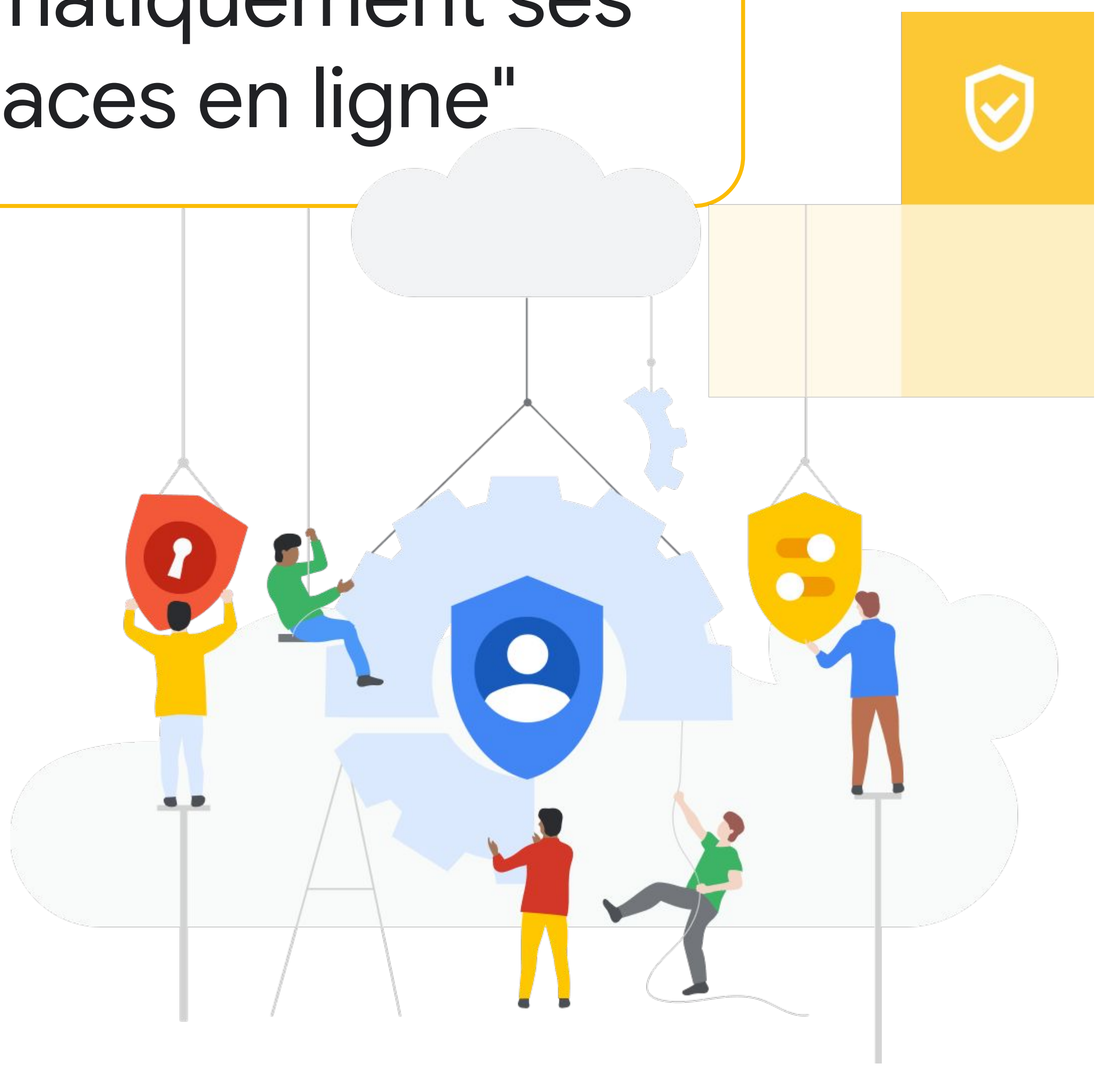
Alors que macOS et Windows 11 permettent aux administrateurs d'installer des logiciels, de créer des utilisateurs et d'apporter d'autres modifications susceptibles de compromettre les données, l'approche de ChromeOS est plus sécurisée.

Avec ChromeOS, il n'existe pas d'utilisateur racine ni d'administrateur, ce qui réduit les chances que le système soit exploité. Même si les utilisateurs peuvent apporter des modifications limitées en mode développeur, ils ne disposent pas des mêmes privilèges qu'un administrateur, ce qui garantit que la surface d'attaque de ChromeOS est réduite par rapport à celle des autres systèmes[1].

chromeOS

4

"ChromeOS protège automatiquement ses utilisateurs contre les menaces en ligne"

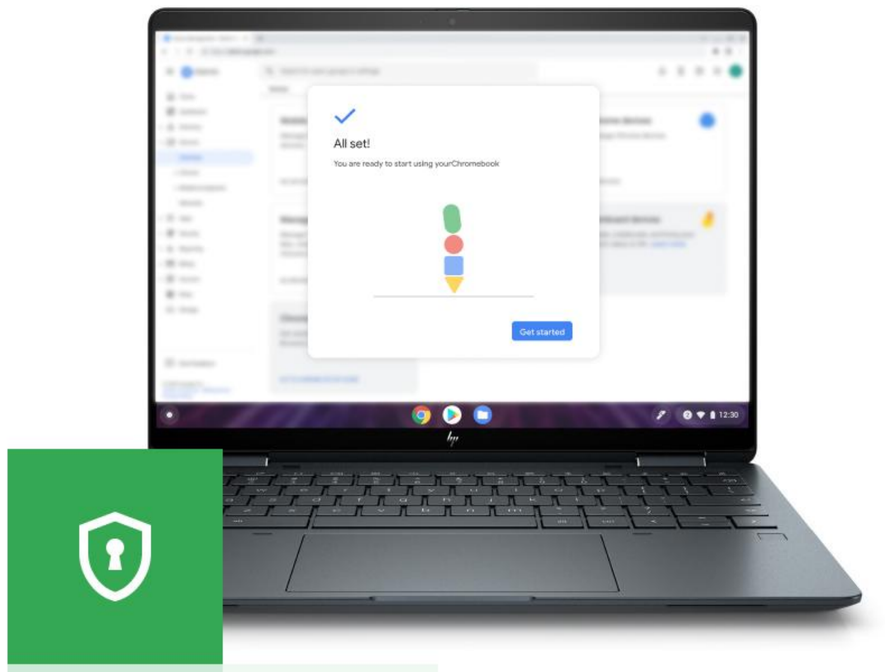


ChromeOS se sert de l'exécution en bac à sable au niveau du système, des applications et du navigateur pour s'assurer que les menaces ciblant vos données sont rapidement neutralisées.

La fonctionnalité de navigation sécurisée intégrée au navigateur Chrome protège automatiquement plus de 5 milliards d'utilisateurs chaque jour en isolant chaque page Web afin qu'elle ne puisse pas agir sur les autres onglets, applis ou éléments de votre appareil. Contrairement à macOS et Windows 11, toute l'architecture du système ChromeOS est segmentée, et les fichiers système essentiels qui ne le sont pas sont complètement isolés. Même si vous accédez à un fichier ou une application malveillants, il ne leur est pas possible d'infiltrer le micrologiciel de votre appareil[1].

5

“Les entreprises et établissements scolaires peuvent contrôler à quoi les utilisateurs ont accès"

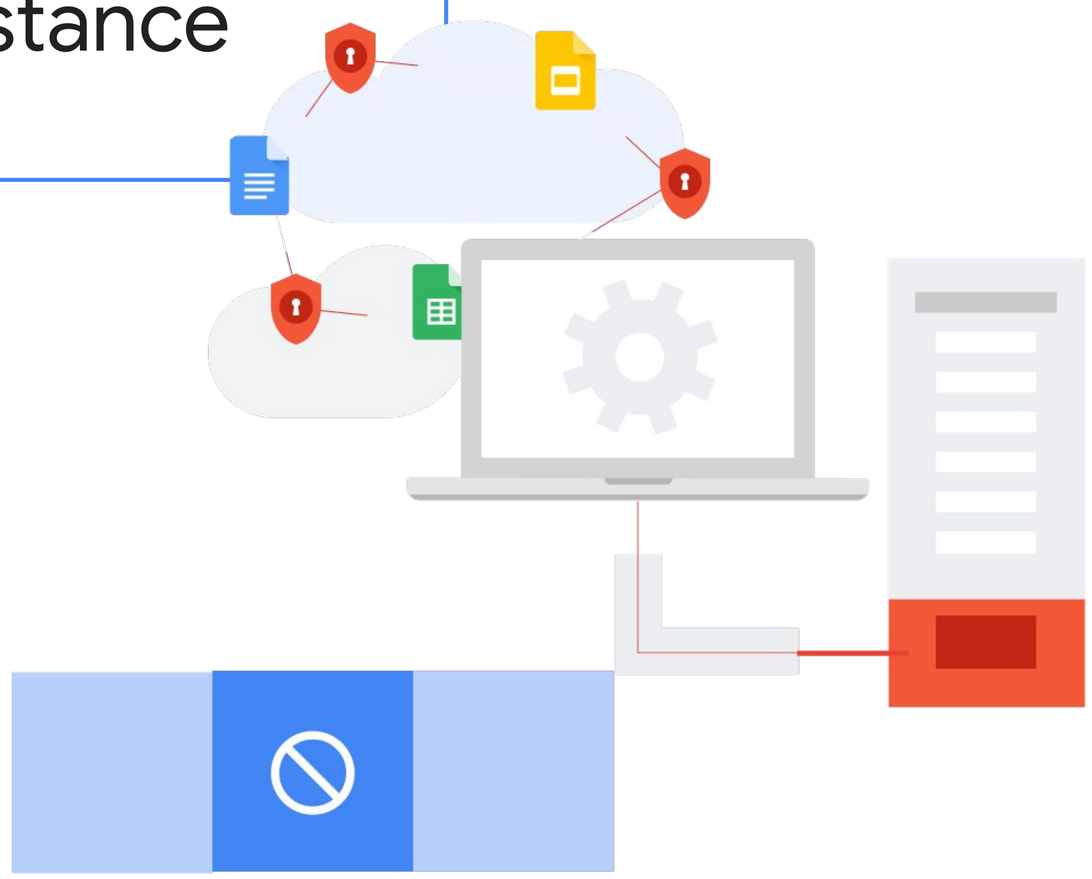


Les Chromebooks sont utilisés chaque jour par 50 millions d'élèves et d'enseignants. ChromeOS s'adapte à ces cas d'utilisation en permettant de restreindre facilement l'accès à des applications et sites Web spécifiques.

La console d'administration Google vous permet de définir des règles qui déterminent à quels contenus Web et extensions l'utilisateur a accès, mais aussi de choisir quels sites sont autorisés à exécuter JavaScript, utiliser des cookies, charger des images et plus encore. Sur macOS et Windows 11, il est bien plus facile de contourner ces contrôles, même lorsque des restrictions sont mises en place[1].

chromeOS

6 "Les pirates informatiques ne peuvent pas accéder à distance aux appareils ChromeOS"

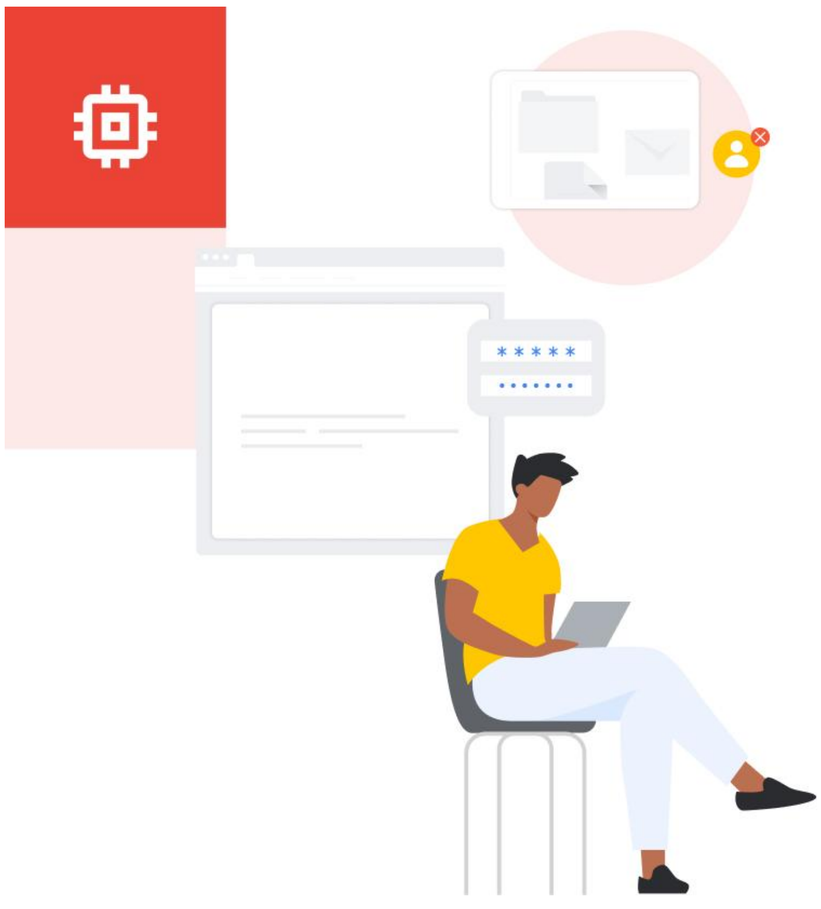


ChromeOS dispose naturellement d'une surface d'attaque à distance réduite.

À l'aide d'un système de pare-feu innovant, ChromeOS empêche les criminels de se servir des protocoles de détection de services pour contaminer les requêtes et forcer les systèmes à se connecter à des ressources qu'ils contrôlent. Bien que macOS et Windows 11 utilisent également de tels pare-feu, ils sont moins efficaces. Les pare-feu de ces deux systèmes d'exploitation sont susceptibles d'être contaminés par le biais de protocoles que celui de ChromeOS bloque[1].

"Avec son comportement par défaut, son grand nombre d'options de configuration et la possibilité pour les applications de modifier leur comportement, ChromeOS apparaît comme la solution la plus efficace pour limiter les surfaces d'attaque à distance[2]."

7 "La puce de sécurité de Google contrecarre les attaques"



Si un pirate informatique souhaite accéder à vos données, il aura besoin d'un accès physique à votre appareil ChromeOS, et sa tâche n'en sera pas pour autant facilitée.

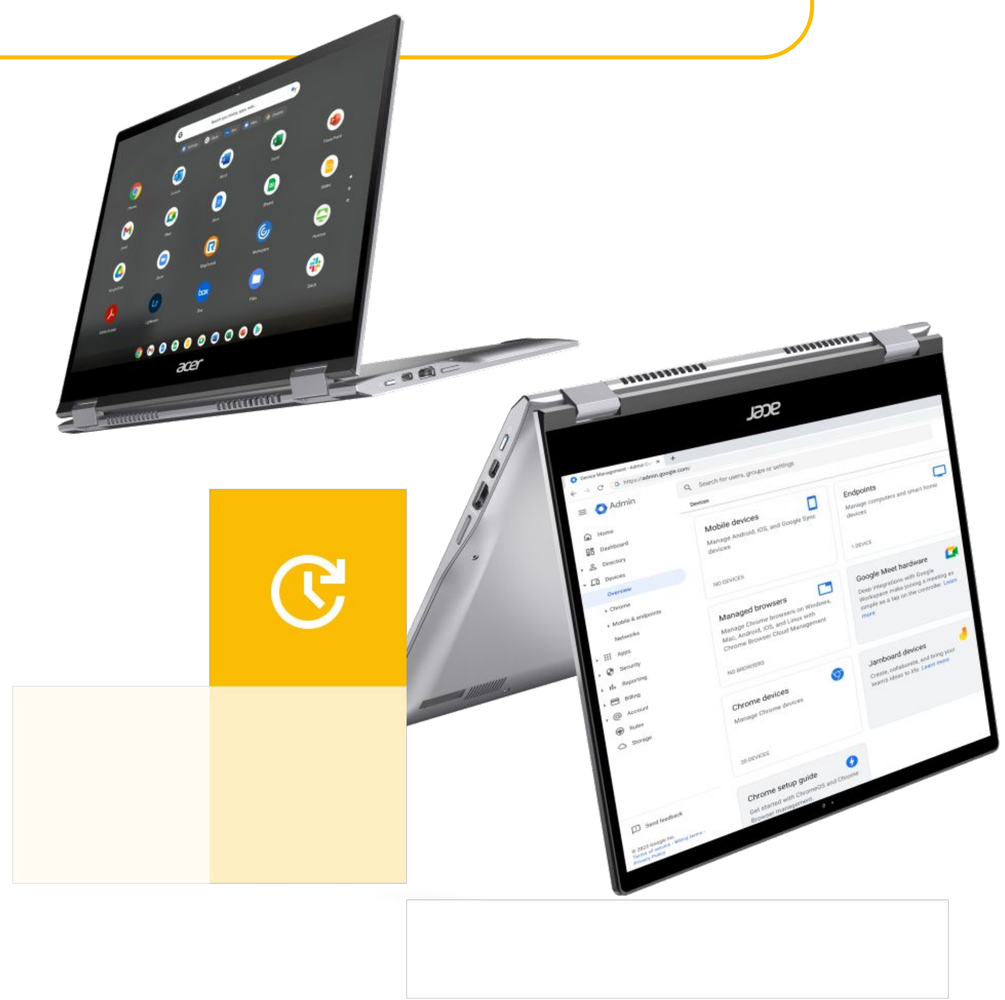
La puce Google Secure Microcontroller (H1) permet le déploiement de nombreuses fonctionnalités de sécurité sur ChromeOS, y compris la protection des clés de chiffrement et des données locales. Même les attaques par force brute, lorsqu'un pirate informatique essaie des millions de combinaisons de mots de passe et de codes pour tenter de se connecter, sont stoppées net par la puce[1].

8

"Avec les mises à jour automatiques, bénéficiez toujours d'une protection de pointe"

Des mises à jour régulières sont nécessaires pour assurer la sécurité des données. Toutefois, elles peuvent devenir chronophages et inutilement compliquées sur certains systèmes d'exploitation.

Sur macOS, les utilisateurs sont parfois obligés d'accepter de nouvelles conditions d'utilisation ou de saisir à nouveau leur mot de passe. Sur Windows 11, les mises à jour automatiques doivent être activées. Alors que sur ChromeOS, les mises à jour sont effectuées automatiquement en arrière-plan par défaut et l'utilisateur est notifié si un redémarrage du système est nécessaire. Puisque le système ChromeOS est conçu pour être hautement intégré, les mises à jour du système s'appliquent à tous les composants en même temps[1].



Vos collaborateurs ne devraient pas avoir besoin de posséder des connaissances approfondies en informatique pour travailler sur le Web de façon sécurisée.

ChromeOS dispose par défaut d'une infrastructure de sécurité avancée basée sur la philosophie zéro confiance, qui s'assure que chaque appareil est instantanément prêt à l'emploi et que votre entreprise passe moins de temps et dépense moins d'argent à configurer des mesures de sécurité supplémentaires.

Consulter l'analyse complète d'Atredis Partners.

Contactez nos experts pour découvrir comment ChromeOS répond aux besoins spécifiques de votre entreprise tout en offrant une expérience plus sécurisée que la concurrence, et ce, dès le premier démarrage[1].

chromeOS

[1] Étude réalisée par Atredis Partners pour le compte de Google, "Google ChromeOS Security Competitive Analysis Report", avril 2024.
[2] En mai 2024, aucune attaque de virus ou de rançongiciel réussie sur les systèmes ChromeOS n'a encore été documentée. Données tirées de diverses bases de données internes et nationales de surveillance de ChromeOS.