FICHE TECHNIQUE

WATCHGUARD FULL ENCRYPTION

La première ligne de défense pour protéger les données simplement et efficacement

Selon Gartner,[1] un ordinateur portable est volé toutes les 53 secondes. Le volume croissant de données stockées sur les postes de travail a manifestement augmenté l'intérêt pour ces données, ainsi que le risque de subir une violation de données par la perte, le vol ou l'accès non autorisé à des informations.

Cela a abouti à un durcissement des réglementations telles que le RGPD[2] dans l'Union européenne et la CCPA[3] aux États-Unis dans l'optique de réduire la probabilité de perte, de vol ou d'accès non autorisé aux données et leurs répercussions économiques considérables.

RENFORCEZ LA SÉCURITÉ CONTRE TOUT ACCÈS NON AUTORISÉ EN CENTRALISANT LA GESTION

L'une des méthodes les plus efficaces pour minimiser l'exposition de vos données consiste à chiffrer automatiquement les disques durs des ordinateurs de bureau, des ordinateurs portables et des serveurs. L'accès aux données est ainsi sécurisé et conforme aux mécanismes d'authentification mis en place. La mise en place de règles de chiffrement fournit une couche de sécurité supplémentaire et de contrôle pour les entreprises, même si cela peut également poser des problèmes de contrôle et de récupération des données en cas de perte de la clé.

WatchGuard Full Encryption utilise BitLocker, une technologie de Microsoft éprouvée et stable, pour chiffrer et déchiffrer les disques durs sans affecter les utilisateurs finaux. Elle permet aux entreprises de centraliser la gestion et le contrôle des clés de récupération stockées sur Aether, la plateforme de gestion dans le Cloud de WatchGuard.

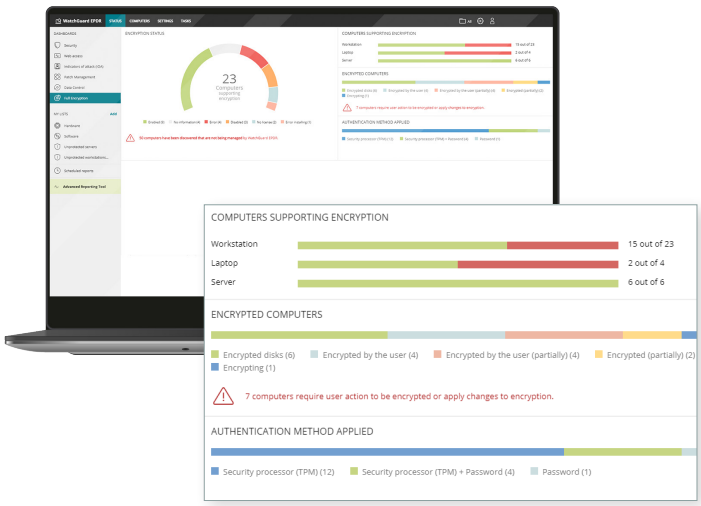


Tableau de bord WatchGuard Full Encryption intégré à la console web de WatchGuard avec des indicateurs clés de l'état de chiffrement des postes de travail de l'entreprise.

AVANTAGES

Évitez la perte ou le vol des données ou l'accès non autorisé à celles-ci sans impacter les utilisateurs.

- Chiffrez vos disques et protégez leurs contenus contre le vol, la perte accidentelle et les intrus malveillants. Le chiffrement des données, le déchiffrement et l'accès sont automatiques, immédiats et simples pour les utilisateurs.
- Pour plus de simplicité, les clés de récupération sont stockées et récupérées en toute sécurité depuis la plateforme Cloud et sa console web.

Pas de déploiement ni installation. Pas de serveur ni frais supplémentaires. Zéro problème.

- **WatchGuard Full Encryption** centralise la gestion de BitLocker, une technologie Windows qui a fait ses preuves et largement utilisée.
- BitLocker est inclus dans la plupart des systèmes d'exploitation Windows. La console web de la plateforme Cloud de WatchGuard vous permet de gérer vos appareils de manière centralisée.
- Vous n'aurez aucun autre agent à déployer ou à installer. Toutes les solutions de protection des postes de travail de WatchGuard Endpoint Security partagent le même agent léger.
- La possibilité de gérer les clés de récupération dans le Cloud évite d'avoir à installer ou à entretenir des serveurs pour les gérer.
- **WatchGuard Full Encryption** peut être activé immédiatement et gérer facilement depuis l'interface utilisateur conviviale de WatchGuard Cloud.

Conformité avec la réglementation, rapports et gestion centralisée

- **WatchGuard Full Encryption** simplifie la mise en conformité avec les réglementations sur la protection des données en surveillant et en activant BitLocker sur les appareils fonctionnant sous Windows.
- Toutes les solutions WatchGuard Endpoint Security fournissent des tableaux de bord intuitifs, des rapports détaillés et les audits de modifications.
- De plus, sa gestion fondée sur des rôles permet aux administrateurs de mettre en place différents niveaux d'autorisation et différentes stratégies pour les groupes et les appareils à partir d'une seule console web.

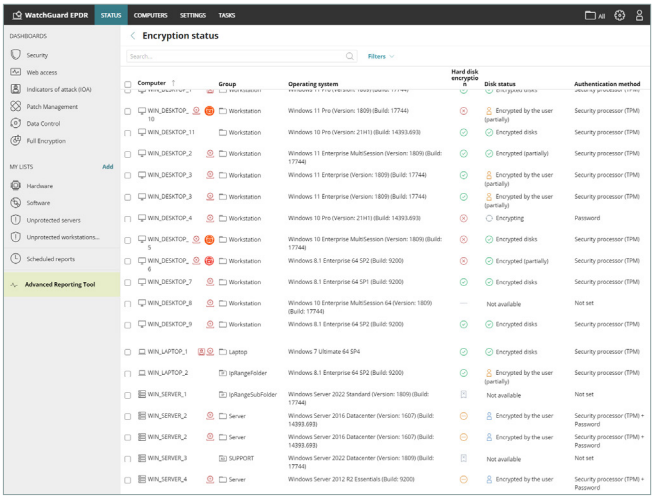
CLÉS USB SÉCURISÉES

L'an dernier, l'utilisation des clés USB dans le monde a progressé de 30 %, notamment dans les entreprises industrielles. Les pirates informatiques s'en sont aperçus et utilisent les clés USB pour accéder aux systèmes et infecter tout ou partie de votre réseau.

Les entreprises ont dès lors plus de chances de subir des violations de données ou des accès non autorisés à des données sensibles. Selon l'étude réalisée par Forrester, [4] la perte ou le vol d'actifs comme les ordinateurs portables ou les clés USB impliquait 20 % de violations de données rapportées par les directeurs de la sécurité du monde entier en 2020.

La première étape visant à minimiser les risques de menaces consiste à disposer d'une stratégie stricte comportant des recommandations pour l'utilisation de clés USB au sein de l'entreprise, les niveaux de rôle et les autorisations basées sur le profil du personnel, en utilisant que les appareils fournis et vérifiés par le service informatique ou le MSP de l'entreprise.

Néanmoins, ces recommandations ne sont peut-être pas suffisantes face à la prolifération des cybermenaces. **WatchGuard Full Encryption** fournit une protection maximale des données sur tous les postes de travail chiffrés en permettant une authentification avant le démarrage qui vérifie l'identité des utilisateurs avant le chargement du système d'exploitation, évitant la perte, le vol des ordinateurs portables et l'accès non autorisé des données.



Liste des ordinateurs indiquant l'état de chiffrement, les groupes auxquels ils appartiennent, leur système d'exploitation et la méthode d'authentification employée.

FONCTIONS CLÉS

La tendance favorable aux modes de travail hybrides, consistant à alterner entre le télétravail et le travail au bureau, fait du chiffrement complet des disques la première ligne de défense cruciale pour les ordinateurs portables et les clés USB.

WatchGuard Full Encryption est un module supplémentaire pour les solutions WatchGuard Endpoint Security. Conçu pour centraliser la gestion du chiffrement complet des disques durs, il offre les fonctions suivantes :

Chiffrement et déchiffrement complets des disques

WatchGuard Full Encryption utilise BitLocker pour chiffrer entièrement les lecteurs de vos ordinateurs portables, ordinateurs de bureau, serveurs et disques de stockage amovibles Windows. Le tableau de bord de **WatchGuard Full Encryption** fournit un aperçu global des postes de travail réseau compatibles, avec leur état de chiffrement et la méthode d'authentification utilisée, et permet aux administrateurs d'attribuer des paramètres de chiffrement et de limiter les autorisations de chiffrement.

Gestion centralisée des clés de récupération

En cas d'oubli de la clé d'accès ou de modification de la séquence de démarrage, BitLocker demande une clé de récupération pour démarrer le système affecté. L'administrateur réseau peut au besoin obtenir la clé de récupération via la console de gestion et l'envoyer à l'utilisateur.

Listes, rapports, application d'une stratégie centralisée

La liste des ordinateurs intégrée à la console permet aux administrateurs d'appliquer différents filtres selon l'état de chiffrement. Ces listes peuvent être exportées pour l'analyse des données avec des outils externes.

Définissez des stratégies de chiffrement à partir de la console et affichez les modifications apportées via des rapports d'audit que vous pouvez au besoin transmettre aux organismes de régulation.

[1] TechSpective

[2] RGPD - Règlement Général Européen sur la Protection des Données : Contraint les entreprises à garantir la protection des informations personnelles qu' elles traitent. Tout non-respect peut être passible de lourdes amendes et de dommages indirects.

[3] CCPA - California Consumer Privacy Act of 2018 : il s' agit de la première loi états-unienne votée dans le sillage du RGPD de l' Union européenne. Elle s' applique aux entreprises basées en Californie et à celles domiciliées en dehors.

[4] The State Of Privacy And Data Protection, 2021 - Forrester

Plateformes prises en charge et configuration système requise pour WatchGuard Full Encryption

Compatible avec les systèmes d'exploitation pris en charge par WatchGuard EPDR, WatchGuard EDR et WatchGuard EPP : Windows.

Liste des navigateurs compatibles : Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge et Opera.

SERVICE COMMERCIAL FRANCE +33 97 755 4336 ADRESSE EMAIL france@watchguard.com SITE INTERNET www.watchguard.com/fr WatchGuard Technologies, Inc.