DATASHEET

WATCHGUARD EPP

Endpoint Protection Platform

DÉFIS EN MATIÈRE DE CYBERSÉCURITÉ

Dans la bataille que vous avez à livrer pour défendre votre entreprise, les postes de travail sont la cible favorite des cybercriminels. D'où l'importance de protéger et surveiller plus que jamais tous les postes de travail qui traitent des informations sensibles et se connectent aux systèmes à l'intérieur comme à l'extérieur du réseau de l'entreprise.

Pas moins de 350 000 programmes malveillants ont été identifiés rien qu'en 2020. Les pirates informatiques jettent leur dévolu sur les postes de travail vulnérables, sur lesquels les entreprises stockent leurs actifs les plus précieux. Pourquoi ? Le plus souvent pour leur soutirer de l'argent. Les malwares et les ransomwares comptent au nombre des menaces les plus répandues, même si paradoxalement, ce ne sont pas tant les coûts directs induits qui posent le plus problème, mais davantage les arrêts de l'activité qu'ils entraînent. Ces interruptions contraignent les entreprises à prendre des mesures pour renforcer leur sécurité.

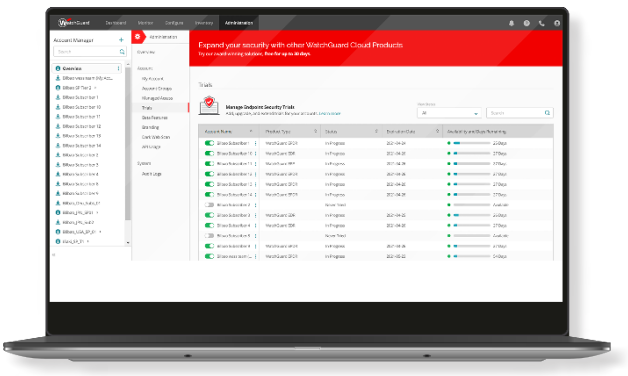
PROTÉGEZ VOTRE ENTREPRISE CONTRE LES MALWARES ET LES RANSOMWARES

L'exposition toujours plus grande des entreprises à de nouveaux types de malwares et de menaces compromet leur sécurité et les oblige à adopter de nouvelles stratégies pour limiter l'impact des possibles attaques.

WatchGuard EPP est une solution de sécurité performante basée dans le Cloud, qui centralise une protection contre les virus de nouvelle génération pour l'ensemble de vos ordinateurs de bureau et portables Windows, macOS et Linux, ainsi que les serveurs, les principaux systèmes de virtualisation et autres appareils iOS y Android. Cette protection complète couvre le réseau (firewall), les emails, le Web et les appareils externes.

Elle comprend un ensemble de technologies EPP conçues pour contrer les malwares, les ransomwares et les dernières menaces. L'une de ces technologies passe au crible en temps réel le vaste référentiel WatchGuard Threat Intelligence alimenté par les derniers algorithmes de Machine Learning afin de détecter plus rapidement les attaques malveillantes.

Vous n'aurez plus non plus à vous soucier de la maintenance du matériel et des logiciels. Son agent léger n'a aucun impact sur les performances des postes de travail, simplifiant ainsi la gestion de la sécurité et améliorant au passage l'efficacité opérationnelle.



AVANTAGES

Sécurité garantie pour plusieurs plateformes

- Protection garantie contre les menaces sophistiquées inconnues : détection et blocage des malwares, des chevaux de Troie, des tentatives d'hameçonnage et des ransomwares.
- Protection contre tous les vecteurs d'attaque : les navigateurs, les emails, les systèmes de fichier et les appareils externes connectés à des postes de travail.
- Analyse automatique des ordinateurs et élimination des virus.
- Analyse comportementale pour détecter les malwares connus et inconnus.
- Solution compatible avec de nombreuses plateformes : Systèmes Windows, Linux, macOS, iOS, Android et environnements virtuels (VMware, Virtual PC, MS Hyper-V, Citrix). Gestion des licences appartenant à une infrastructure de virtualisation persistante et non-persistante.

Simplifiez la gestion

- Maintenance simplifiée : aucune infrastructure particulière requise pour héberger la solution ; le service informatique de l'entreprise peut se concentrer sur les tâches les plus importantes.
- Protection des utilisateurs distants simplifiée : chaque ordinateur protégé par la solution WatchGuard EPP communique avec le Cloud ; les bureaux et les utilisateurs distants sont protégés rapidement et facilement, sans avoir à installer d'autres solutions ou logiciels.
- Déploiement simplifié : plusieurs méthodes de déploiement, avec des programmes de désinstallation automatique pour les produits concurrents afin de faciliter et accélérer la migration à partir de solutions de tiers.
- Courbe d'apprentissage rapide : interface d'administration intuitive, simple et en ligne, avec les options les plus utilisées à portée de clic.

Moins d'impact sur les performances

- L'agent consomme très peu de bande passante, de mémoire et de puissance de traitement, car toutes les opérations sont réalisées dans le Cloud.
- WatchGuard EPP évite d'avoir à installer, à administrer ou à maintenir de nouvelles ressources matérielles au sein de l'infrastructure de l'entreprise.

SÉCURITÉ CENTRALISÉE DES APPAREILS

Gestion centralisée des mises à jour de sécurité et produits pour tous les postes de travail et les serveurs connectés au réseau de l'entreprise. Gérez la protection des appareils fonctionnant sous Windows, Linux, macOS, iOS et Android à l'aide d'une console d'administration en ligne.

PROTECTION CONTRE LES MALWARES ET LES RANSOMWARES

WatchGuard EPP analyse les comportements et les technologies de piratage pour détecter et bloquer les malwares, qu'ils soient connus ou non, ainsi que les ransomwares, les chevaux de Troie et les attaques par hameçonnage.

DÉSINFECTION AVANCÉE

En cas de brèche de sécurité, la solution WatchGuard EPP permet aux entreprises de restaurer rapidement les ordinateurs infectés à l'état qui était le leur avant l'attaque grâce à des outils de désinfection et de mise en quarantaine, qui stockent les éléments suspects et supprimés.

La solution permet également aux administrateurs de redémarrer les postes de travail et les serveurs à distance afin de s'assurer que les dernières mises à jour produits ont été installées.

MONITORING EN TEMPS RÉEL ET RAPPORTS

Des tableaux de bord complets et des graphiques faciles à interpréter permettent une surveillance approfondie et en temps réel de l'intégrité des systèmes.

Des rapports sur l'état de la protection, les menaces détectées et toute utilisation inappropriée des appareils sont générés automatiquement et transmis.

CONFIGURATION ULTRA-FINE DES PROFILS

Attribuez des stratégies de protection en fonction du profil utilisateur, de manière à garantir l'application de la stratégie la plus adaptée à chaque catégorie d'utilisateurs.

CONTRÔLE CENTRALISÉ DES APPAREILS

Dites adieu aux malwares et aux fuites d'informations en bloquant des catégories entières d'appareils (clés USB, modems USB, webcams, DVD/CD, etc.), en autorisant des appareils ou en configurant des autorisations d'accès en lecture seule, en écriture seule et en lecture et en écriture.

INSTALLATION RAPIDE ET FLEXIBLE

Installez la protection par email en utilisant une adresse URL de téléchargement ou installez la solution discrètement sur certains postes de travail à l'aide de l'outil de distribution prévu à cet effet. Le programme d'installation MSI est compatible avec les outils de tiers (Active Directory, Tivoli, SMS, etc.).

MALWARE FREEZER

Malware Freezer isole les malwares détectés pendant sept jours et restaure automatiquement le fichier infecté sur le système en cas de fausse alerte.

REMÉDIATION DES RANSOMWARES ET RÉCUPÉRATION

Pour empêcher la récupération d'un système corrompu, hormis en chiffrant ses fichiers, les adversaires essaient de supprimer les fichiers de sauvegarde et VSS créés par les administrateurs et de désactiver les services de récupération de ces fichiers.

La fonctionnalité de clichés instantanés exploite la technologie des systèmes d'exploitation et protège ces fichiers grâce à notre technologie de protection contre les falsifications, afin que les utilisateurs puissent récupérer leurs informations suite à une attaque de ransomware.

Les experts informatiques utilisent des clichés instantanés pour récupérer des fichiers suite à d'importantes défaillances du système. Cette technologie permet également de récupérer des fichiers chiffrés par un ransomware.

Plateformes prises en charge et configuration système requise pour WatchGuard EPP

Systèmes d'exploitation pris en charge : Windows (Intel et ARM), macOS (Intel et ARM), Linux et Android.

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.