



WatchGuard Endpoint Security

Protection modulable pour prévenir les menaces sophistiquées, les détecter et y répondre

Le poste de travail est une cible privilégiée des cybercriminels en raison de ses nombreuses vulnérabilités connues exploitables et de ses versions logicielles souvent dépassées. Ces appareils sont souvent connectés à Internet sans être protégés par le périmètre de sécurité de l'entreprise, et pire encore, les employés peuvent involontairement permettre aux pirates informatiques de se frayer un chemin jusqu'aux postes de travail et réseaux de l'entreprise. L'époque où les entreprises de toutes tailles devaient mettre en œuvre une sécurité robuste pour leurs postes de travail, associant une protection des postes de travail (EPP) et des technologies avancées de détection et de réponse aux menaces au niveau des postes de travail (EDR), est révolue.

La plateforme de sécurité des postes de travail WatchGuard offre une protection maximale avec une complexité minimale, éliminant toute incertitude en ce qui concerne la sécurité des postes de travail. Nos produits et services de sécurité centrés sur les utilisateurs offrent des approches EPP et EDR de pointe, avec une suite complète d'outils de sécurité et d'exploitation conçue pour protéger les personnes, les appareils et les réseaux auxquels elles se connectent contre les sites Web malveillants, les malwares, le spam et autres attaques ciblées. Reposant sur des processus automatisés propulsés par l'IA et sur des services d'investigation assurés par des analystes en sécurité, nos produits WatchGuard EPDR et WatchGuard EDR proposent le service Threat Hunting et une classification totale, certifiant la légitimité et la sécurité de toutes les applications exécutées : un besoin essentiel pour toute entreprise qui met en œuvre un modèle de sécurité de type Zero-Trust.

Bienveillant ou malveillant ? En avoir le cœur net

La plupart des produits de sécurité pour les postes de travail bloquent les programmes connus comme étant malveillants, enquêtent sur les programmes suspects et autorisent les programmes inconnus, permettant ainsi aux malwares qui mutent rapidement de contourner les défenses en place. En revanche, les produits WatchGuard EDR et WatchGuard EPDR intègrent le service Zero-Trust Application qui classe 100 % des fichiers exécutables en analysant tous les processus et applications inconnus à l'aide d'algorithmes de Machine Learning spécifiques au sein de notre plateforme Cloud, et même en les vérifiant avec nos techniciens de laboratoire, le cas échéant. Ainsi, tous les fichiers exécutables sont connus comme étant des goodwares ou des malwares, ce qui permet aux clients de recevoir seulement des alertes avérées et de profiter de la protection ultime provenant du postulat de refus par défaut typique d'une approche Zero-Trust.

Détectez les menaces qui rodent sans ajouter de personnel

La traque des menaces requiert généralement des ressources humaines très qualifiées, et de nombreuses heures peuvent être nécessaires pour les détecter et remonter les informations qui permettent de savoir précisément comment y remédier. Nos solutions EDR de pointe assurent un service de Threat Hunting dans le cadre duquel nos analystes de sécurité surveillent l'environnement des postes de travail du client et fournissent des informations concernant les potentielles attaques en cours, notamment une analyse des causes principales, les anomalies détectées, des données informatiques pertinentes et de potentielles propositions visant à réduire la surface d'attaque. Il s'agit d'une fonctionnalité standard proposée avec nos produits WatchGuard EDR et WatchGuard EPDR, qui évite au personnel informatique des entreprises d'avoir à consacrer du temps et de l'énergie à enquêter sur les postes de travail infectés.

Profitez d'une gestion dans le Cloud intuitive

Les entreprises qui possèdent un personnel informatique et une expertise en sécurité limitée tireront parti de tous les avantages offerts par WatchGuard Cloud. La plateforme de gestion dans le Cloud simplifie le déploiement, la configuration ainsi que la gestion de vos produits de sécurité des postes de travail. Elle offre une protection et une communication en temps réel avec les postes de travail intégrant notre moteur de sécurité et nos signatures, ainsi qu'un filtrage des URL qui permet aux utilisateurs de déployer des tâches et des configurations sur des milliers d'ordinateurs en quelques secondes. Par ailleurs, WatchGuard Cloud vous permet de gérer l'ensemble de votre portefeuille de façon centralisée, réduisant ainsi les coûts d'infrastructure et minimisant le temps consacré au reporting et aux tâches opérationnelles.

Étendez votre sécurité, votre visibilité et vos capacités d'exploitation

Des modules facultatifs sont disponibles avec tous les produits de sécurité EPP et EDR. Profitez de Patch Management pour gérer de façon centralisée les mises à jour et correctifs pour les systèmes d'exploitation d'applications tierces et de programmes logiciels non pris en charge (EOL), déployez Full Encryption pour chiffrer et déchiffrer des informations sur les postes de travail, utilisez notre outil Advanced Reporting Tool pour générer des informations relatives à la sécurité, identifier les attaques et les comportements inhabituels, et ajoutez Data Control pour identifier, classer, analyser et surveiller les données personnelles non structurées stockées sur les postes de travail. SIEM Feeder vous offre une nouvelle source d'informations stratégiques sur l'ensemble des processus qui s'exécutent sur vos appareils. Notre outil de surveillance et de gestion à distance Systems Management permet quant à lui de gérer, de surveiller et de préserver votre infrastructure informatique.

Un package complet doté d'options flexibles pour répondre à tous les besoins spécifiques

WatchGuard EDR et WatchGuard EPDR

- Une solution de détection et de réponse au niveau des postes de travail (EDR) assure une solide protection contre les attaques de type « Zero Day », les ransomwares, le cryptojacking et d'autres attaques ciblées sophistiquées grâce à des modèles d'IA, nouveaux et émergents, reposant sur le Machine Learning et le Deep Learning.
- Options possibles : EDR uniquement (WatchGuard EDR) et EPP + EDR (WatchGuard EPDR).
Bénéficiez d'un service de classification à 100 % avec Zero-Trust Application Service, pour créer le type de réponse requis dans le cadre du déploiement d'un modèle Zero-Trust.
Augmentez l'utilisation et l'efficacité du personnel grâce aux données fournies par le service de traque des menaces (Threat Hunting).
- Pour vos postes de travail, mettez en œuvre une sécurité assurant une défense en profondeur avec WatchGuard EPDR, qui réunit tous les avantages de notre produit de détection et de réponse au niveau des postes de travail ainsi que de notre produit Endpoint Protection au sein d'un seul ensemble.

WatchGuard EPP

- Une protection des postes de travail contre les virus, les malwares, les logiciels espions et le phishing grâce à des signatures, une mémoire cache locale et même nos propres flux d'intelligence dérivés des malwares détectés précédemment par les produits WatchGuard EDR et WatchGuard EPDR.
- WatchGuard s'adresse aux organisations prenant en charge un large éventail d'appareils. WatchGuard EPP centralise la protection antivirus de nouvelle génération pour l'ensemble de vos ordinateurs de bureau et ordinateurs portables Windows, macOS et Linux, ainsi que des serveurs, en plus des principaux systèmes de virtualisation et des appareils Android & iOS. Notre solution vous permet de centraliser la gestion de la sécurité et de la confidentialité des données stockées sur les smartphones et tablettes Android & iOS des utilisateurs.
- Une détection des attaques de type « Zero Day » à l'aide d'analyses heuristiques et comportementales, et d'indicateurs d'attaques (IoA) connus comme des « règles contextuelles ».

Modules de sécurité supplémentaires

Ajoutez les modules optionnels disponibles avec tous les produits de sécurité EPP et EDR:

WatchGuard Patch Management

WatchGuard Patch Management est une solution qui permet de gérer de manière centralisée les mises à jour et les correctifs appliqués aux systèmes d'exploitation et aux centaines d'applications tierces et de programmes logiciels non pris en charge car arrivés en fin de vie (EoL).

WatchGuard Full Encryption

WatchGuard Full Encryption s'appuie sur la technologie Microsoft BitLocker pour chiffrer et déchiffrer les informations des postes de travail et centraliser la gestion des clés de chiffrement stockées sur notre plateforme de gestion dans le Cloud.

Effectuez une extension avec plus de modules optionnels disponibles uniquement avec les produits WatchGuard EPDR et WatchGuard EDR:

WatchGuard Advanced Reporting Tool

WatchGuard Advanced Reporting Tool génère automatiquement des informations relatives à la sécurité et fournit les outils nécessaires pour identifier les attaques et les comportements inhabituels et détecter les abus internes susceptibles de survenir sur le réseau de l'entreprise.

WatchGuard Data Control*

WatchGuard Data Control* identifie, classe, analyse et surveille les données personnelles non structurées stockées sur les postes de travail et les serveurs tout au long de leur cycle de vie.

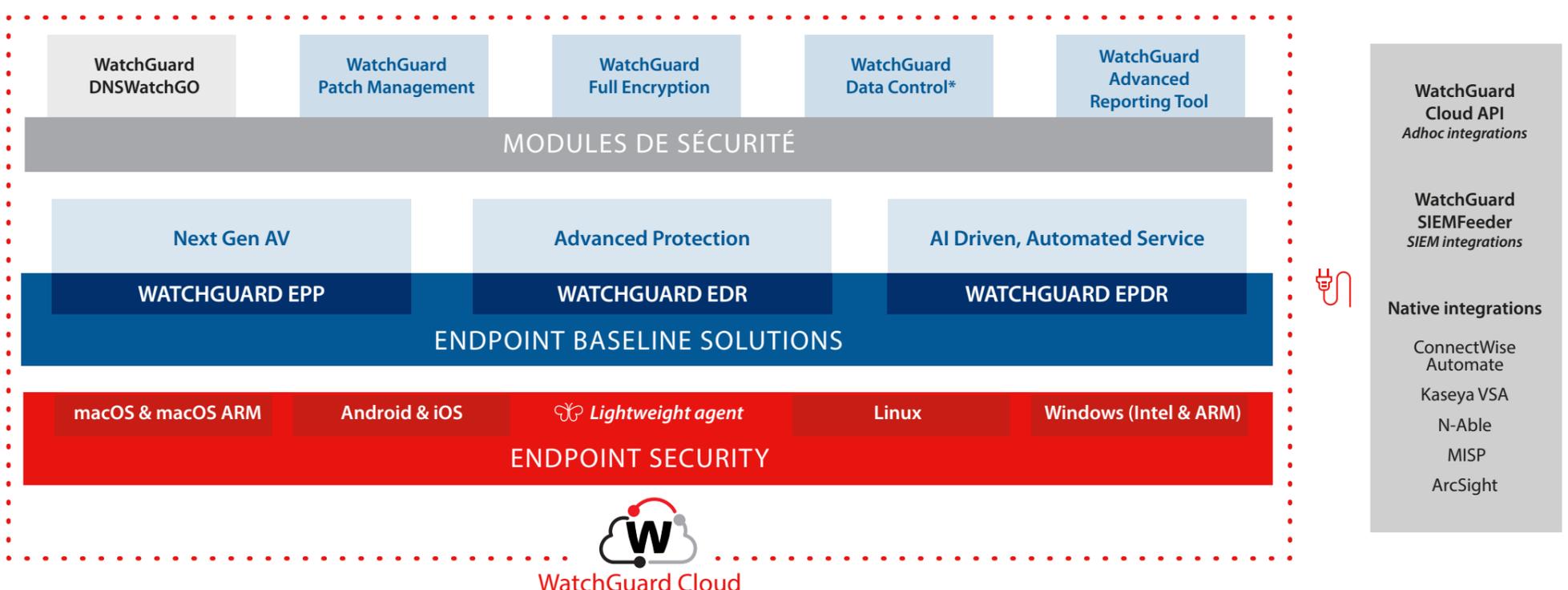
**Data Control est disponible dans les pays suivants : Espagne, Allemagne, Royaume-Uni, Suède, France, Italie, Portugal, Hollande, Finlande, Danemark, Suisse, Norvège, Autriche, Belgique, Hongrie et Irlande.*

WatchGuard SIEMFeeder

WatchGuard SIEMFeeder vous offre une nouvelle source d'informations stratégiques sur la sécurité de l'ensemble des processus qui s'exécutent sur vos appareils et sont surveillés en continu.

WatchGuard DNSWatchGO

WatchGuard DNSWatchGO assure une protection et un filtrage du contenu au niveau du DNS pour protéger les entreprises contre les attaques telles que le phishing et les ransomwares, même lorsque les utilisateurs se trouvent en dehors du réseau, sans avoir besoin d'un VPN.



Pourquoi vous devez mettre à niveau votre sécurité

1. Pour protéger les télétravailleurs dispersés à mesure que les politiques de télétravail des entreprises se développent.

WatchGuard Passport comprend WatchGuard EPDR, WatchGuard DNSWatchGO et WatchGuard AuthPoint pour l'authentification multifacteur. Ces solutions se combinent pour protéger les utilisateurs contre le plus large éventail de menaces qui soit. En plus d'assurer la sécurité des postes de travail, elles protègent les ressources de l'entreprise contre les infiltrations dues à la perte ou au vol des identifiants des employés : un vecteur d'attaque mis à profit dans le cadre de certaines des plus grandes failles publiées.



★ Solution recommandée : **WatchGuard Passport**

2. Pour vous remettre d'une attaque ou après la découverte d'un malware latent sur des postes de travail ou des réseaux de l'entreprise lorsque le malware provient d'un poste de travail.

Les entreprises qui sont dans cette situation savent deux choses : premièrement, qu'elles présentent certainement un intérêt pour les cybercriminels, et deuxièmement, que leur niveau de protection actuel est inadapté. À mesure que la protection avancée de WatchGuard EPDR a évolué avec l'ajout de Zero-Trust Application Service et de Threat Hunting Service, le nombre d'attaques de malware sur lesquelles notre équipe de support a enquêté/auxquelles elle a remédié a eu tendance à se rapprocher de zéro, ce qui signifie que nos clients n'en ont pas fait l'âpre expérience. Combinez cela avec des outils de visibilité et de gestion afin de renforcer la productivité d'une équipe informatique surmenée, et vous aurez tout l'arsenal nécessaire pour éviter des attaques répétées et des mesures de remédiation coûteuses.

★ Solution recommandée : **WatchGuard EPDR**

3. Pour ajouter une solution EDR à une solution antivirus existante en tant qu'investissement de sécurité planifié.

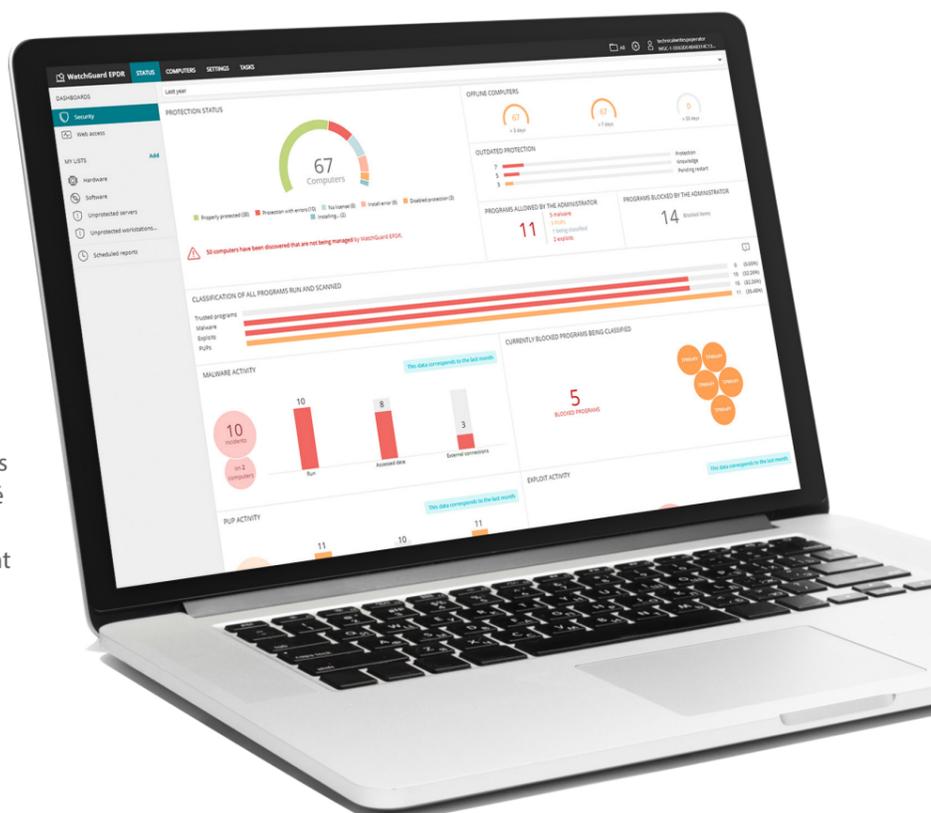
Conscientes des risques de sécurité que comportent leurs postes de travail, ces entreprises ont déployé un produit antivirus mais se rendent compte qu'elles ont également besoin d'une solution EDR pour garder une longueur d'avance sur les pirates informatiques. Il est inutile d'attendre le renouvellement de contrat d'un antivirus. Notre solution WatchGuard EDR se superpose à un déploiement antivirus existant afin que les clients puissent bénéficier rapidement de notre approche innovante.

★ Solution recommandée : **WatchGuard EDR**

4. Pour passer d'un produit antivirus gratuit ou grand public pour les postes de travail à un produit plus avancé.

Parfois, les entreprises de petite taille ou qui possèdent peu d'appareils qui traversent le périmètre réseau misent sur un profil de risque réduit et remettent donc à plus tard leurs investissements en matière de sécurité. Cependant, le monde évolue, et comme les entreprises sont de plus en plus exposées et doivent se conformer à des réglementations plus strictes en matière de confidentialité et de sécurité des données, elles n'hésitent pas à adopter une solution de niveau professionnel comme le produit WatchGuard EPP. Proposant une prévention basée sur les signatures, notamment les signatures des malwares présents dans notre base installée, ainsi qu'une analyse des comportements, un filtrage du contenu Web, WatchGuard EPP est un choix judicieux et durable dans la mesure où la plateforme évolue au rythme de la croissance de l'entreprise.

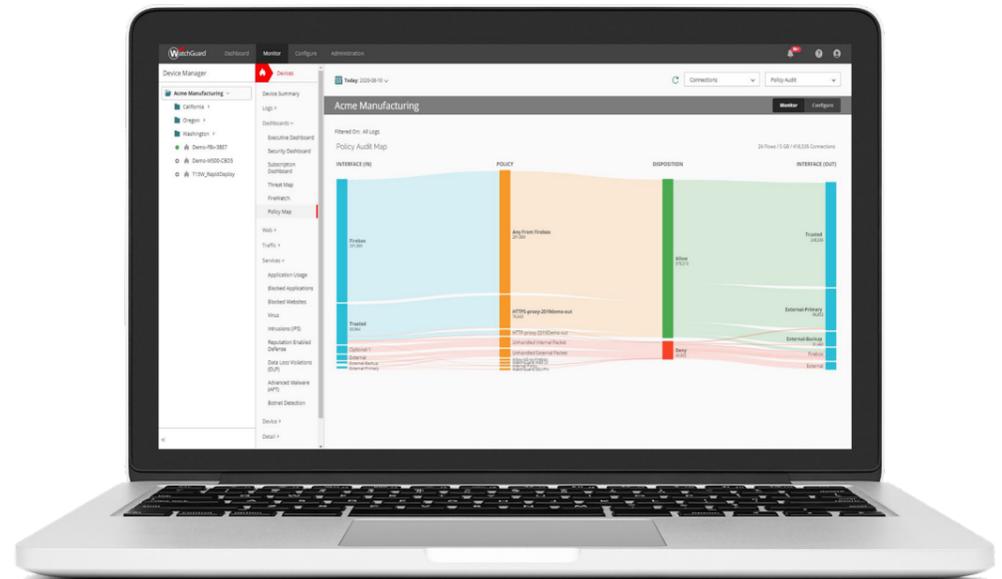
★ Solution recommandée : **WatchGuard EPP**



WatchGuard Cloud



- Connectez-vous en temps réel pour déployer des tâches sur des milliers d'appareils en quelques secondes
- Gérez tous les produits de la marque WatchGuard à partir d'une console unique
- Visualisez des appareils sur toutes les plateformes des postes de travail, notamment Windows, Linux, macOS, iOS et Android



CATALOGUE DE WATCHGUARD



Sécurité réseau

Les solutions de sécurité réseau WatchGuard sont spécifiquement conçues pour être faciles à déployer, à utiliser et à gérer, en plus d'offrir la meilleure sécurité qui soit. Notre approche novatrice de la sécurité réseau s'efforce de fournir une protection de pointe à toutes les entreprises, indépendamment de leur taille et de leur niveau d'expertise technique.



Authentification multifacteur

WatchGuard AuthPoint® permet de combler la faille de sécurité qu'induit le recours à des mots de passe au moyen d'une authentification multifacteur, via une plateforme Cloud facile à utiliser. L'approche unique de WatchGuard se démarque grâce au facteur « ADN de téléphone portable » qui permet de vérifier que seules les personnes autorisées ont accès aux réseaux et aux applications Cloud sensibles.



Wi-Fi Cloud sécurisé

Conçues pour offrir un environnement Wi-Fi de confiance sécurisé, éliminant les tâches d'administration fastidieuses et réduisant considérablement les coûts, les solutions de Wi-Fi sécurisé WatchGuard changent littéralement la donne sur le marché actuel. Avec des outils d'engagement exhaustifs et une parfaite visibilité sur vos données d'entreprise, cette solution confère à votre entreprise un avantage concurrentiel indéniable.



Sécurité des postes de travail

WatchGuard Endpoint Security est une gamme Cloud native de pointe qui assure la sécurité des postes de travail et protège les entreprises contre toutes les cyberattaques, actuelles et futures. Sa solution phare reposant sur l'intelligence artificielle, WatchGuard EPDR, améliore instantanément la posture des entreprises en matière de sécurité. Elle associe des capacités de protection des postes de travail (EPP) et de détection et de réponse au niveau des postes de travail (EDR) avec Zero-Trust Application Service et Threat Hunting Service.

En savoir plus

Pour plus d'informations, contactez un revendeur agréé WatchGuard ou consultez notre site à l'adresse suivante : <https://www.watchguard.com/fr>.

À propos de WatchGuard

WatchGuard® Technologies, Inc. est leader mondial en matière de sécurité et d'intelligence réseau, de Wi-Fi sécurisé, d'authentification multifacteur et de sécurité des postes de travail. Les produits et les services primés de WatchGuard sont recommandés par plus de 18 000 revendeurs et prestataires de services spécialisés dans la sécurité, et protègent plus de 250 000 clients à travers le monde. WatchGuard a pour mission d'offrir une sécurité de pointe aux entreprises de tous types et de toutes tailles, ce qui en fait la solution idéale pour les PME et les entreprises multisites. L'entreprise a établi son siège social à Seattle, dans l'État de Washington, et possède des bureaux en Amérique du Nord, en Europe, en Asie-Pacifique et en Amérique latine. Pour en savoir plus, rendez-vous sur le site [WatchGuard.com/fr](https://www.watchguard.com/fr).