FICHE TECHNIQUE

WATCHGUARD EPDR

Endpoint Protection Detection and Response

DÉFIS ORGANISATIONNELS EN MATIÈRE DE CYBERSÉCURITÉ

Les postes de travail sont la cible principale de la plupart des cyberattaques, et alors que l'infrastructure technologique se complexifie, les entreprises peinent à trouver l'expertise et les ressources nécessaires pour surveiller et gérer les risques de sécurité inhérents aux postes de travail. Alors, à quels types de défis les entreprises sont-elles confrontées lorsqu'elles adoptent des solutions de sécurité des postes de travail ?

- **Désensibilisation aux alertes :** les entreprises reçoivent des milliers d'alertes de malware par semaine, dont seulement 19 % sont considérées comme fiables, et 4 % sont examinées. Les administrateurs cybersécurité consacrent généralement les deux tiers de leur temps à la gestion des alertes de malware.
- **Complexité :** lorsque les outils de cybersécurité déconnectés sont trop nombreux, les professionnels de la sécurité peuvent se retrouver en difficulté à cause du nombre de technologies mises en œuvre, de l'absence de connaissances internes et du temps requis pour identifier les menaces.
- **Performance insuffisante :** les solutions de sécurité des postes de travail fréquemment utilisées nécessitent l'installation et la gestion de plusieurs agents sur chaque ordinateur de bureau, serveur et ordinateur portable surveillé, ce qui entraîne de graves erreurs, une mauvaise performance et une consommation élevée des ressources.

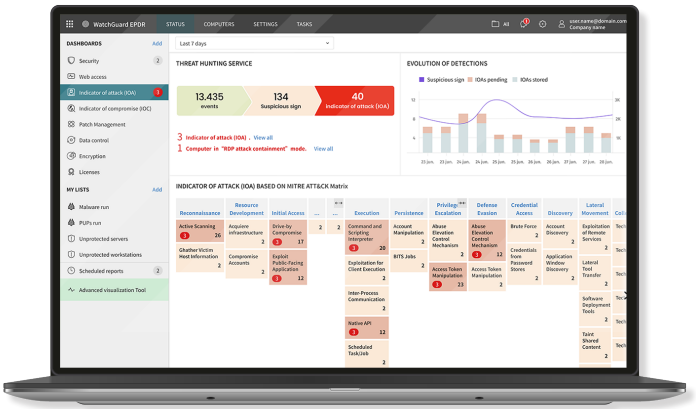
Les techniques traditionnelles de protection des postes de travail (EPP), qui mettent l'accent sur la prévention, sont adaptées aux menaces et aux comportements malveillants connus, mais elles sont insuffisantes pour les cybermenaces sophistiquées.

DE LA PRÉVENTION À LA RÉPONSE – SÉCURITÉ AUTOMATISÉE DES POSTES DE TRAVAIL

La solution WatchGuard EPDR est une solution de cybersécurité innovante dans le Cloud pour les ordinateurs de bureau, les ordinateurs portables et les serveurs. Elle automatise la prévention, la détection, le confinement des menaces sophistiquées, des malwares de type Zero Day, des ransomwares, des attaques de type phishing, des exploits de mémoire et des autres attaques

Contrairement aux autres solutions, elle combine le plus large éventail de technologies de protection des postes de travail (EPP) avec des capacités de détection et de réponse (EDR) automatisées. Elle comprend également deux services, gérés par les experts de WatchGuard, qui sont aussi intégrés à la solution:

- **Service Zero-Trust Application :** Classification de la totalité des applications
- **Service Threat Hunting :** détection des pirates informatiques et des attaques venant de l'intérieur.



La solution WatchGuard EPDR regroupe un antivirus nouvelle génération et des technologies EDR et de protection innovantes et évolutives dans une seule et même solution permettant aux professionnels de l'informatique de contrer des cybermenaces avancées.

Technologies antivirus nouvelle génération

- Firewall personnel ou géré, système de détection des intrusions (IDS)
- Contrôle des appareils
- Intelligence collective et analyses heuristiques avant exécution
- Anti-malware multi-vectoriel permanent et analyse à la demande
- Filtrage des URL, navigation sur Internet et anti-hameçonnage
- Protection contre les falsifications
- Remédiation automatique et capacité de restauration
- Évaluation des vulnérabilités

Technologies de sécurité avancées

- Surveillance continue des postes de travail avec EDR
- Machine Learning dans le Cloud permettant de classer l'intégralité des processus (APT, ransomwares, rootkits, etc.)
- Sandbox dans des environnements réels
- Protection anti-exploit
- Protection contre les attaques réseau : prévention des attaques exploitant les vulnérabilités des services accessibles sur Internet
- Traque des menaces : analyse des comportements et détection des indicateurs d'attaque (IoA) afin de détecter les attaques LotL (Living-off-The-land).
- Indicateurs d'attaque associés au dispositif MITRE ATT&CK
- Détection et prévention des attaques RDP
- Fonctionnalités de confinement et de remédiation comme l'isolation de l'ordinateur et le blocage des programmes selon le hachage ou le nom

AVANTAGES

Simplifie et maximise la sécurité

- Des services automatisés réduisent les coûts liés au personnel expert. Vous n'avez aucun faux positif à traiter, vous ne perdez pas de temps à configurer manuellement les paramètres et aucune tâche n'est déléguée.
- La performance des endpoints n'est pas impactée puisqu'elle repose sur un agent unique et une architecture dans le Cloud.

Utilisation et gestion simplifiées

- La gamme Endpoint Security répond à tous les besoins de protection de vos postes de travail de manière extrêmement simple depuis une console Web unique.
- La configuration est facile. Gestion des postes de travail sur plusieurs plateformes depuis un seul et même écran.

Fonctionnalités EDR uniques

- Conservation des données pendant 12 mois et sandboxing en temps réel permettant d'éviter que les tentatives de piratage ne passent inaperçues.
- Service Zero-Trust Application : chaque processus est classifié en fonction de son comportement dynamique. Service de traque des menaces : détection des pirates informatiques et des attaques venant de l'intérieur.

MODÈLE ZERO-TRUST : PLUSIEURS COUCHES DE PROTECTION

La plateforme de sécurité des postes de travail de WatchGuard ne s'appuie pas sur une seule technologie, mais sur plusieurs, afin que les auteurs des menaces ne puissent pas arriver à leurs fins. Lorsqu'elles fonctionnent en symbiose, ces technologies utilisent les ressources au niveau du poste de travail pour limiter le risque de faille.

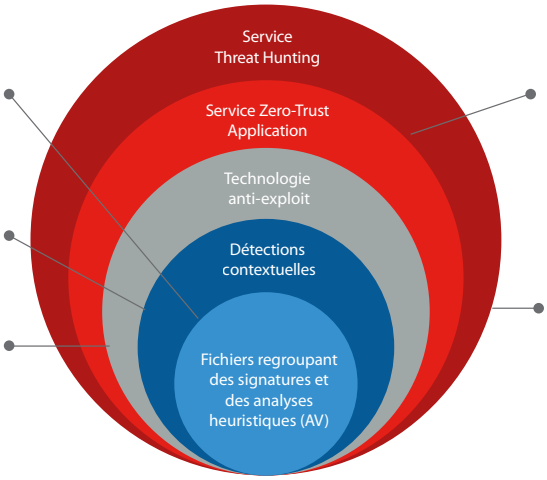
Modèle « Zero-Trust » : Plusieurs couches de protection

COUCHES POUR LES POSTES DE TRAVAIL :

Couche 1/ Fichiers regroupant des signatures et technologies d'analyse heuristique
Une technologie optimisée, efficace pour détecter les attaques connues

Couche 2 / Détections contextuelles
Elles nous permettent de détecter les attaques sans malware et sans fichier

Couche 3 / Technologie anti-exploit
Elle nous permet de détecter les attaques sans fichier qui visent à exploiter les failles



COUCHES SPÉCIALEMENT CONÇUES POUR LE CLOUD

Couche 4 / Service Zero-Trust Application
Permet de détecter lorsqu'une couche précédente subit une atteinte, neutralise les attaques sur des ordinateurs déjà infectés et bloque les attaques par mouvement latéral à l'intérieur du réseau

Couche 5 / Service Threat Hunting
Détectez les endpoints compromis, les attaques dès les premiers stades de leur exécution ainsi que les activités suspectes, et identifiez les indicateurs d'attaque qui minimisent les temps de détection et de réponse (MTTD et MTTR).

METTEZ EN PLACE UNE SÉCURITÉ ROBUSTE ET SIMPLIFIÉE AVEC UNIFIED SECURITY PLATFORM DE WATCHGUARD

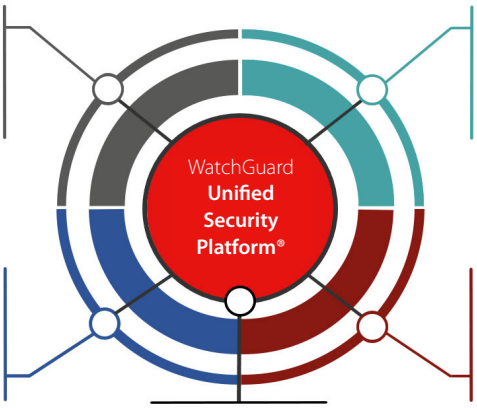
L'architecture Unified Security Platform de WatchGuard est une plateforme unique pour améliorer la sécurité moderne. Notre approche de la plateforme vous aide à fournir des services de sécurité robustes pour chaque vecteur de menace avec une vitesse accrue, tout en soutenant l'efficacité opérationnelle et une plus grande rentabilité.

SÉCURITÉ DE BOUT EN BOUT

Un portefeuille complet de produits et de services de sécurité qui protègent les environnements, les utilisateurs et les appareils : **endpoints, authentification multifacteur et sécurité réseau.**

CLARTÉ ET CONTRÔLE

Centralisation de la gestion de la sécurité, de la visibilité et de la génération de rapports avancés via **WatchGuard Cloud**.



ALIGNEMENT OPÉRATIONNEL

Des opérations commerciales simplifiées avec un accès direct aux API, un riche écosystème d'**intégrations** prêtes à l'emploi et la prise en charge de tous les modèles de paiement et de consommation via **FlexPay**.

CONNAISSANCES PARTAGÉES

Une plateforme entièrement intégrée pour adopter une posture Zero Trust en matière de sécurité via WatchGuard **Identity Framework**, et déployer une véritable approche fondée sur XDR pour la détection et la remédiation des menaces via **ThreatSync®.**

AUTOMATISATION

WatchGuard Automation Core® apporte une simplification et une mise à l'échelle à chaque aspect du delivery et de la gestion de la sécurité.

Plateformes prises en charge et configuration système requise pour WatchGuard EPDR

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

Les fonctionnalités EDR sont disponibles sur Windows, macOS et Linux. Seul Windows permet de bénéficier de l'ensemble des fonctionnalités.

Liste des navigateurs compatibles : Google Chrome, Mozilla Firefox, Safari et Microsoft Edge.

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