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.

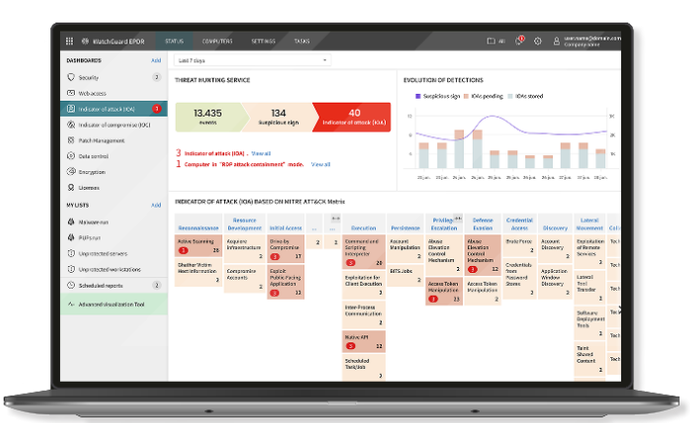
Les techniques traditionnelles de protection des postes de travail (EPP), qui mettent l'accent sur la prévention, sont adaptées aux menaces et aux comportements malveillants connus, mais elles sont insuffisantes pour les cybermenaces sophistiquées. Des vecteurs de piratage les plus courants aux nouvelles menaces, les cybercriminels sont toujours à la recherche de nouveaux moyens pour échapper au radar des services informatiques, contourner les mesures de protection et exploiter de nouvelles failles.

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 sans malware et sans fichier, ainsi que la réponse face à ceux-ci, au sein du réseau de l'entreprise comme en dehors.

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 des technologies endpoint traditionnelles 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 cyber-menaces avancées :

Technologies de prévention traditionnelles

- Firewall personnel ou géré, système de détection des intrusions (IDS)
- Contrôle des appareils
- Veille collective
- Liste de refus / Liste d'autorisation
- Anti-malware multi-vectoriel permanent et analyse à la demande
- Analyses heuristiques avant exécution
- Filtrage des URL – navigation sur Internet
- Anti-hameçonnage
- Protection contre les falsifications
- Remédiation automatique et capacité de restauration
- Récupération de fichiers chiffrés grâce à des clichés instantanés

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
- Traque des menaces (Threat Hunting), dont l'analyse des comportements et la détection des indicateurs d'attaque pour déceler 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.
- Pas d'installation, de configuration ni de maintenance d'une infrastructure de gestion.
- Agent léger et architecture dans le Cloud : la performance des postes de travail n'est pas impactée.

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.
- Elle fournit une interface utilisateur épurée et intuitive qui se maîtrise rapidement.

Fonctionnalités EDR automatisées

- Détecte et bloque les techniques, tactiques et procédures de piratage, et les activités malveillantes au niveau de la mémoire (exploits) avant qu'elles ne puissent faire des dégâts.
- Résolution des problèmes et réponse aux menaces : données criminalistiques permettant d'examiner chaque tentative d'attaque, et outils pour en limiter les effets (désinfection).
- Traçabilité de chaque action : visibilité concrète sur l'attaquant et ses activités, simplifiant ainsi les analyses criminalistiques.

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.

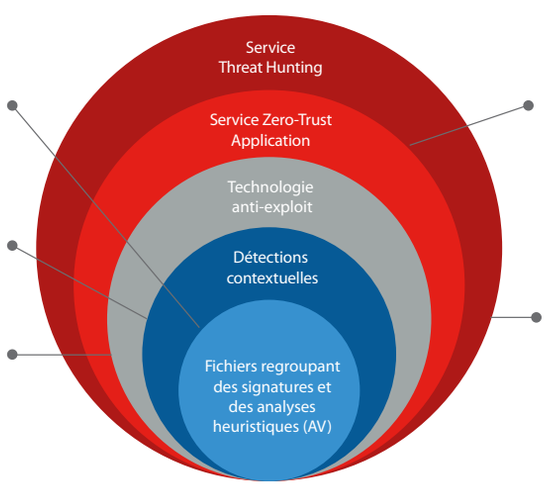
Modèle « Zero-Trust » : Plusieurs couches de protection

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
Nous permet de détecter les postes de travail compromis, les attaques à un stade précoce, les activités suspectes et les indicateurs d'attaque

Les fichiers de signatures et technologies d'analyse heuristique, appelés « Protection traditionnelle des endpoints » (EPP), constituent une couche technologique composée d'un antivirus nouvelle génération qui est efficace contre la plupart des menaces connues de bas niveau et améliore le blocage des URL malveillantes.

La détection contextuelle est très efficace contre les attaques basées sur des scripts, les attaques utilisant des outils du système d'exploitation (goodware), tels que PowerShell, WMI, etc., ainsi que les failles des navigateurs et d'autres applications souvent ciblées, telles que Java, Adobe Reader, etc.

La technologie anti-exploit recherche et détecte tout comportement anormal. Elle revêt une importance stratégique pour les endpoints vulnérables/en attente de correctifs, ainsi que pour les endpoints utilisant des systèmes d'exploitation qui ne sont plus pris en charge.

Zero-Trust Application Service classe 100 % des processus, en bloquant par défaut toute exécution jusqu'à ce qu'elle soit certifiée comme étant de confiance. Inutile de classer manuellement les menaces ou de les déléguer à des administrateurs chargés de la sécurité.

Threat Hunting Service repose sur un ensemble de règles de traque des menaces établies par des experts en cybersécurité. Celles-ci sont automatiquement appliquées à toutes les données collectées à partir de la télémétrie, ce qui déclenche des indicateurs d'attaque dont le rôle est de minimiser le temps de détection (MTTD) et le temps de réponse (MTTR).

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.

La prise en charge des systèmes existants commence à partir de Windows XP SP3 et Server 2003.

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, Internet Explorer, Microsoft Edge et Opera.

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