DATASHEET

WatchGuard EDR

Détection et réponse au niveau des endpoints

Défense basée sur l'IA contre les menaces sophistiquées

Les solutions traditionnelles en matière de protection des endpoints et d'antivirus, bien qu'essentielles pour se défendre contre les malwares connus, ne fournissent pas la visibilité et les technologies avancées nécessaires à la détection précoce de ce type d'attaques et à leur réponse automatisée. Avec l'affinement toujours plus poussé des méthodes des cyberattaquants, on constate une augmentation de la fréquence et de la complexité des cybermenaces.

Les solutions de sécurité des endpoints traditionnelles génèrent souvent des alertes de faible priorité qui pèsent sur les administrateurs informatiques et de sécurité, les obligeant à gérer et à classer manuellement les menaces. En plus d'engendrer davantage de stress, elles font courir un risque de négligence des alertes critiques.

Renforcez votre cybersécurité : passez à une solution automatisée

WatchGuard EDR est une solution de cybersécurité basée dans le Cloud pour plusieurs appareils. Elle automatise la prévention, la détection et le confinement des menaces avancées telles que les malwares de type « Zero Day », les ransomwares, le phishing, les exploits de mémoire, ainsi que la réponse adéquate face à ces menaces. Offrant une visibilité complète des endpoints, WatchGuard EDR détecte et arrête les cyberattaques que les solutions de sécurité traditionnelles ne parviennent pas à repérer.

WatchGuard EDR s'intègre parfaitement aux solutions antivirus existantes, améliorant votre infrastructure de sécurité avec un ensemble complet de capacités EDR et de services managés, dont :

- **le service Zero-Trust Application qui offre une classification de la totalité des applications ; et**
- **le service Threat Hunting qui détecte les pirates informatiques et les attaques venant de l'intérieur de l'entreprise ciblée.**

Fonctionnalités clés

- Détection des menaces basée sur l'IA : utilise des technologies d'IA et de Machine Learning dans le Cloud pour classer l'intégralité des processus et des applications.
- Sandbox physique : permet d'effectuer une analyse comportementale sur les applications dans des environnements sécurisés pour déceler les menaces.
- Protection anti-exploits : protège contre les attaques basées sur des exploits.
- Protection contre les attaques réseau : prévient les attaques exploitant les vulnérabilités des services accessibles sur Internet.
- Détection des indicateurs d'attaque : permet de conduire des analyses basées sur le framework MITRE ATT&CK™ fournissant des indicateurs d'attaque afin d'atténuer les menaces en cours et de prévenir les attaques futures.
- Détection et prévention des attaques RDP : assure la sécurité contre les attaques de protocole de bureau à distance.
- Confinement et remédiation : comprend des fonctionnalités telles que le blocage des programmes et l'isolement des périphériques.
- Récupération de fichiers : récupère les fichiers chiffrés à l'aide de clichés instantanés.

Avantages

Simplifie la sécurité et réduit les coûts afférents à la sécurité

- Services managés réduisant le besoin de personnel expert et éliminant les fausses alertes, en veillant à ce qu'aucune responsabilité ne soit déléguée.
- Gestion des endpoints compatible avec de nombreuses plateformes de façon centralisée.
- Agent léger et architecture Cloud native évitant les répercussions au niveau des performances des endpoints.

Automatise et réduit le délai de détection

- Blocage des applications à risque selon le hachage ou le nom.
- Prévention de l'exécution de malwares de type « Zero Day », d'attaques sans fichier, de ransomwares et de phishing.
- Détection et blocage des techniques, tactiques et procédures de piratage.

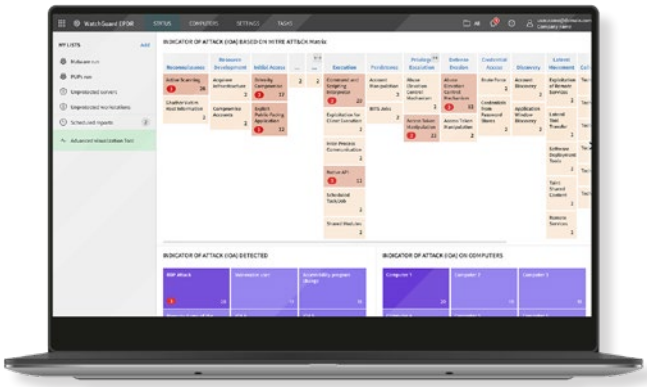
Réduction du temps de réponse et d'analyse

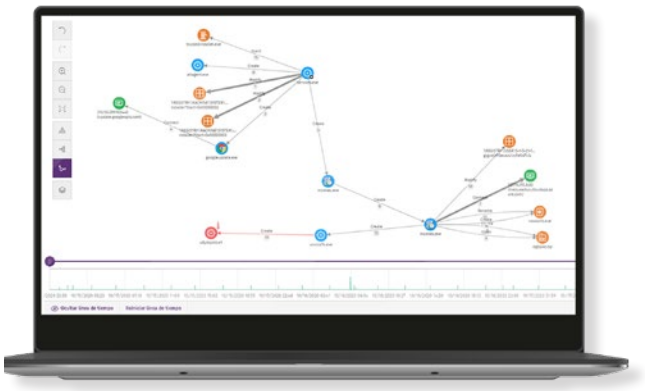
- Transmission de données criminalistiques permettant de mener des enquêtes approfondies et d'atténuer les effets des attaques (élimination des virus).
- Accès à une visibilité concrète au niveau des activités des attaquants et des enquêtes avancées en matière d'indicateurs d'attaque.
- Amélioration des politiques de sécurité basée sur les conclusions de l'analyse criminalistique.

Zero-Trust et Threat Hunting

La sécurité des endpoints WatchGuard ne s'appuie pas sur une seule technologie. Nous en mettons plusieurs en œuvre pour réduire les chances de réussite des auteurs de menace. Ces technologies fonctionnent conjointement et utilisent les ressources de l'endpoint afin de minimiser les risques de faille.

Le **service Zero-Trust Application** classe l'intégralité des processus, surveille les activités sur les endpoints et bloque l'exécution des applications et des processus malveillants. Chaque exécution est catégorisée en temps réel comme malveillante ou légitime, en toute certitude et sans intervention manuelle, en tirant parti des technologies d'IA et du traitement Cloud pour évolutivité l'évolutivité et l'adaptabilité.

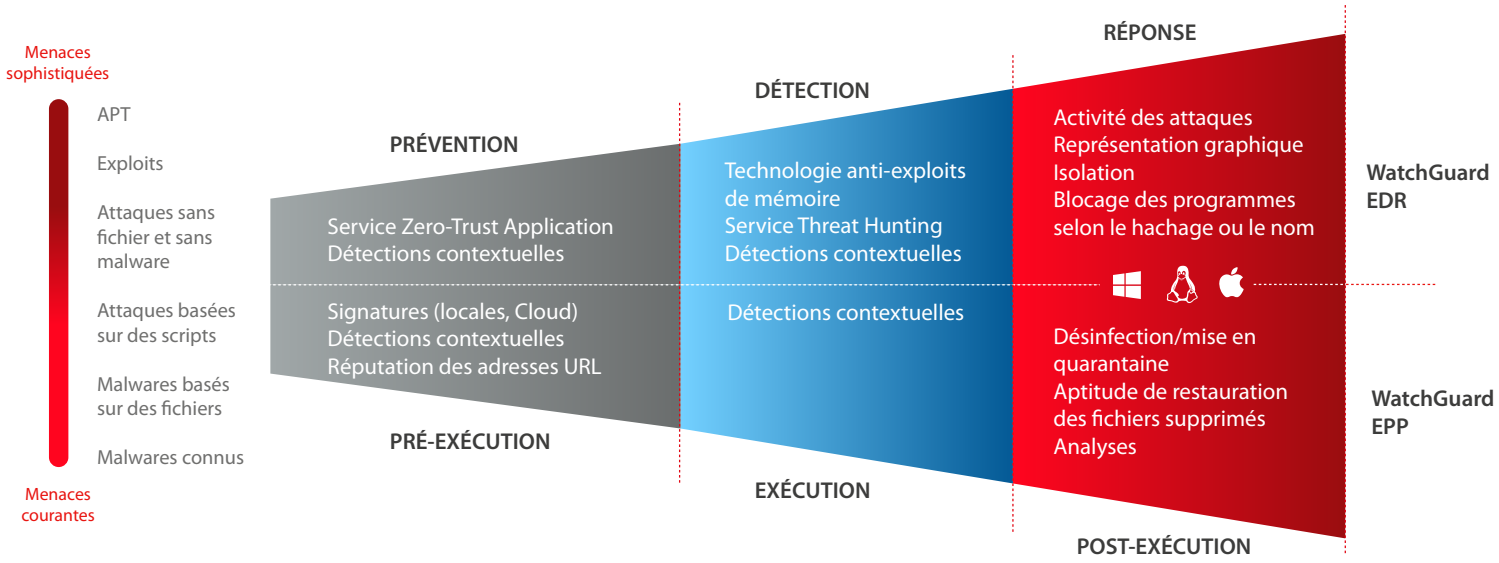




Le **service Threat Hunting** utilise des règles créées par des spécialistes de la cybersécurité et appliquées à toutes les données collectées à partir de la télémétrie pour déclencher des indicateurs d'attaque de haute confiance avec un minimum de faux positifs. Ce processus continu utilise des analyses avancées, des informations internes sur les menaces et des analyses d'experts pour découvrir et minimiser le temps de détection (MTTD) et le temps de réponse (MTTR), en partant du principe que les entreprises sont constamment ciblées.

Une sécurité EDR complète pour ne plus laisser passer de menaces

Mettez votre sécurité à niveau avec WatchGuard EDR. Améliorez votre antivirus traditionnel avec des fonctionnalités EDR de pointe pour garder une longueur d'avance sur les menaces sophistiquées. Grâce à ses fonctionnalités automatisées de détection, de réponse et de monitoring en continu, WatchGuard EDR offre une protection complète de vos appareils, de vos utilisateurs et de vos données. Nos services uniques Zero-Trust Application et Threat Hunting aident à minimiser l'impact des défis en matière de cybersécurité moderne, assurant une sécurité robuste et proactive pour votre entreprise. Sécurisez votre avenir dès aujourd'hui.



Plateformes prises en charge et configuration système requise pour WatchGuard EDR

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

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, Microsoft Edge et Safari.

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