Fiche technique

# WatchGuard APT Blocker

## PROTECTION CONTRE LES LOGICIELS MALVEILLANTS AVANCÉS ET LES ATTAQUES ZERO DAY

Les entreprises qui s'appuient uniquement sur les logiciels antivirus ne sont plus protégées. Ce qui rend les menaces actuelles tellement dangereuses est le fait qu'elles peuvent aisément se déguiser en code qui passe inaperçu auprès des produits basés sur signature qui recherchent un modèle de logiciel malveillant reconnaissable.

### Solution sandbox de nouvelle génération pour une émulation système complète

WatchGuard APT Blocker se concentre sur l'analyse des comportements pour déterminer si un fichier est malveillant. APT Blocker identifie et signale les fichiers suspects à une sandbox de prochaine génération basée sur le Cloud, un environnement virtuel dans lequel le code est analysé, émulé et exécuté pour déterminer son potentiel de menace.

Les menaces avancées, notamment les APT (menaces persistantes avancées), sont conçues pour reconnaître les modes de détection et s'en cacher. L'émulation système complète d'APT Blocker (qui simule le matériel physique, notamment le processeur et la mémoire) offre le plus haut niveau de visibilité du comportement des logiciels malveillants et s'avère être le plus difficile à détecter par les logiciels malveillants avancés.

### Types de fichiers analysés par APT Blocker

- Tous les fichiers exécutables Windows
- Fichiers Adobe PDF
- Fichiers Microsoft Office, notamment Excel, Word, Visio, PowerPoint
- Fichiers Android Application Installer (.apk)

Les fichiers compressés, tels que les fichiers Windows .zip, sont décompressés.

**LE ZERO DAY EST LE NOUVEAU CHAMP DE BATAILLE**

Il n'existe aucun correctif logiciel et aucune signature pour les attaques zero day.

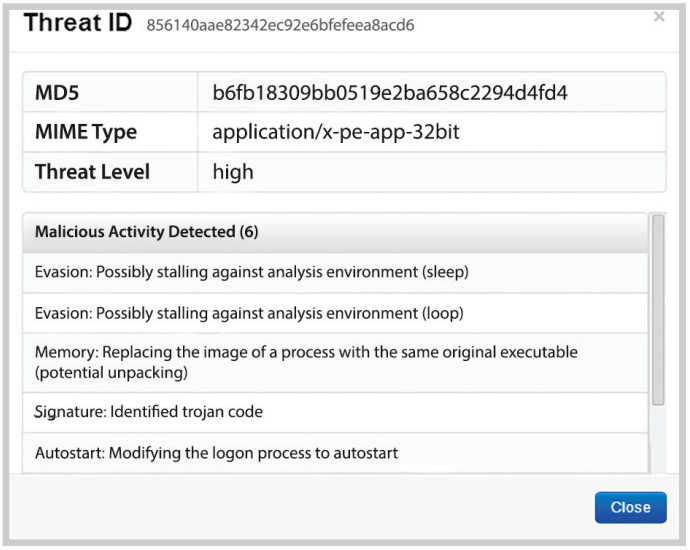
Les solutions antivirus basées sur les signatures restent une première ligne de défense essentielle, en éliminant les menaces au niveau de la passerelle.

APT Blocker étend la protection du monde des logiciels malveillants connus à celui des logiciels malveillants inconnus, assurant ainsi la sécurité de votre entreprise contre les menaces actuelles en perpétuelle évolution.

**Près de 88 %** des logiciels malveillants actuels peuvent **prendre une autre forme pourne pas être détectés** par les solutions antivirus basées sur les signatures...

*« Malwise », IEEE Computers*

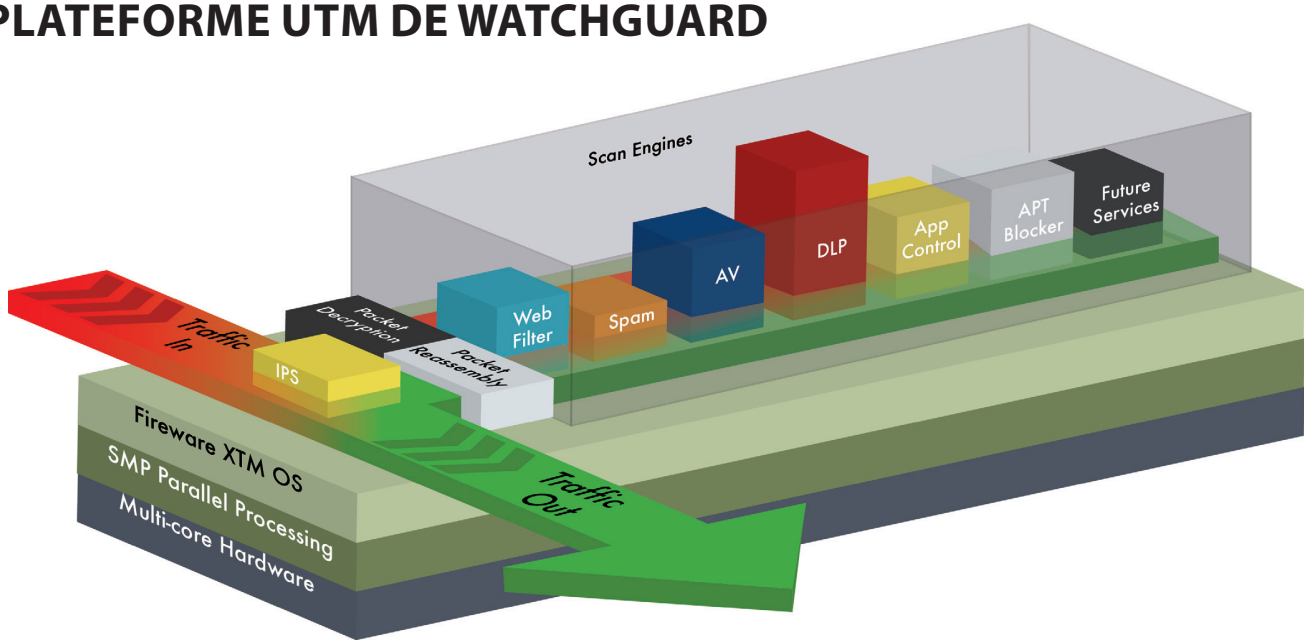
### Bien plus qu'une simple détection, une visibilité sans précédent




Un rapport sur les APT illustre en détail l'activité de logiciels malveillants pour expliquer comment un fichier est identifié en tant que logiciel malveillant

Non seulement APT Blocker offre un niveau de protection inégalé contre les logiciels malveillants avancés, mais il le fait de manière simple et intuitive. Grâce à WatchGuard Dimension™, inclus sans frais supplémentaire dans chaque appliance WatchGuard XTM et chaque solution Firebox®, vous bénéficiez d'une protection efficace contre les attaques zero day, mais également d'une visibilité en temps réel et d'informations faciles à comprendre sur les menaces qui impactent vos réseaux.

# PLATEFORME UTM DE WATCHGUARD




**Son architecture flexible bloque les menaces transmises par le réseau tout en optimisant les performances**

La plateforme UTM de WatchGuard a été conçue pour faire passer le trafic réseau à travers une suite complète de services de sécurité, de la protection contre les e-mails non sollicités à la prévention des pertes de données, en conférant au processus des niveaux de performance exceptionnels. En exploitant la puissance du traitement multicœur, la plateforme exécute simultanément tous les moteurs d'analyse, assurant une protection optimale et un débit ultrarapide. Les ressources sont allouées en fonction du flux de données et des services de sécurité requis par ces données. Par exemple, si le filtrage Web a besoin de plus de puissance, des processeurs supplémentaires y sont automatiquement alloués pour que le trafic Internet reste fluide et votre entreprise protégée.

## LA GESTION DES ABONNEMENTS EST UN JEU D'ENFANT

Toutes les fonctionnalités de sécurité de votre solution WatchGuard XTM ou Firebox T10, y compris les abonnements de sécurité, peuvent être gérées depuis une seule et même console intuitive.

### SACHEZ À TOUT MOMENT CE QUI SE PASSE SUR VOTRE RÉSEAU

- Toute activité de sécurité identifiée par un service est journalisée et stockée afin de simplifier la création de rapports et vous permettre de prendre immédiatement des mesures préventives ou correctives.
- Tous les outils de gestion, y compris la surveillance et la création de rapports détaillés, sont inclus dans votre achat de pare-feu WatchGuard. Aucun achat de matériel ou de logiciel supplémentaire n'est nécessaire.

## COMMENT ACHETER

Les services de sécurité de WatchGuard sont disponibles sous la forme d'abonnements d'un an ou de plusieurs années. Pour en savoir plus sur comment ajouter les meilleures défenses du marché à votre appliance WatchGuard, y compris des services groupés et des promotions spéciales, contactez votre revendeur WatchGuard ou envoyez-nous un e-mail sur france@watchguard.com.

## LA MEILLEURE SOLUTION UTM DE SA CATÉGORIE

WatchGuard utilise le meilleur de chaque technologie pour délivrer les solutions de sécurité les plus fiables du marché. En s'associant aux fournisseurs de solutions technologiques leaders de leur secteur, WatchGuard peut proposer une gamme de services de sécurité véritablement unique.

- **AVG** : Toujours placé en tête des tests antivirus indépendants, il fournit le moteur de notre antivirus de passerelle.
- **Cyren** : sa technologie RPD® brevetée pour le Cloud permet à notre service spamBlocker d'être la seule solution anti-spam efficace pour les appliances UTM. Jusqu'à 4 milliards de messages analysés par jour.
- **Websense** : fournit la base de données d'URL basée sur le Cloud pour notre service WebBlocker. Notre couverture de sécurité est complétée par les laboratoires de sécurité Websense et leur réseau ThreatSeeker.
- **Trend Micro** : l'un des principaux fournisseurs de services IPS et de signatures d'application qui offre une protection complète contre les toutes dernières menaces.
- **Sophos** : l'un des principaux fournisseurs de solutions de sécurité pour le courrier électronique, postes de travails et terminaux mobiles, y compris des solutions DLP, pour les entreprises du monde entier.
- **Lastline** : fournit l'analyse d'émulation système complète, basée sur le Cloud, et la détection avancée des évasions sur lesquelles repose APT Blocker.

SERVICE COMMERCIAL FRANCE 01 40 90 30 35 SERVICE COMMERCIAL INTERNATIONAL +1.206.613.0895 www.watchguard.fr