GoSecure TITAN

ANTIVIRUS DE NOUVELLE GÉNÉRATION GOSECURE TITAN[MC] (NGAV) 2024

L'Antivirus de nouvelle génération GoSecure TitanMC (NGAV) offre une sélection convaincante de fonctionnalités, bien au-delà des antivirus traditionnels, mais couvrant toujours les bases de cette technologie de sécurité éprouvée. Alors que certains vous diront que l'AV traditionnel est obsolète, GoSecure estime que vous avez besoin d'une solide combinaison d'antivirus traditionnels et de nouvelle génération pour protéger rapidement et efficacement les points finaux. Les fichiers malveillants tirant parti des exploits via des attaques sans fichier sont la nouvelle norme. La détection et la protection contre ces attaques à multiples facettes nécessitent plusieurs approches en matière de sécurité des points finaux, et le NGAV GoSecure TitanMC est à la hauteur.

ANTIVIRUS DE NOUVELLE GÉNÉRATION

Remplacez les solutions antivirus existantes par la dernière technologie antimaliciel sur les points finaux pour faire face aux attaques émergentes, sans fichier, basées sur la mémoire et bien plus encore.

APPRENTISSAGE AUTOMATIQUE

Tous les produits GoSecure sont soutenus par notre apprentissage automatique leader du secteur. Développé pour offrir la meilleure qualité et la corrélation la plus rapide possible, l'apprentissage automatique de GoSecure est en constante révision pour maintenir des résultats de la plus haute fidélité.

ANALYSEUR DE MÉMOIRE AVANCÉ

L'analyseur de mémoire avancé surveille le comportement d'un processus malveillant et l'analyse une fois qu'il est déconnecté de la mémoire. Les logiciels malveillants sans fichier fonctionnent sans avoir besoin de composants persistants dans le système de fichiers qui peuvent être détectés de manière conventionnelle. Seule l'analyse de la mémoire permet de découvrir et d'arrêter ces attaques malveillantes.

BOUCLIER CONTRE LES RANÇONGICIELS

Le bouclier contre les rançongiciels est une couche supplémentaire protégeant les utilisateurs contre les rançongiciels. Cette technologie surveille et évalue toutes les applications exécutées en fonction de leur comportement et de leur réputation. Elle est conçue pour détecter et bloquer les processus dont le comportement s'apparente à celui d'un rançongiciel.

GESTION POUR L'OPTIMISATION

La technologie en elle-même constitue une première étape solide, mais que se passe-t-il avec toutes les informations (c.-à-d. les alertes) fournies par la technologie ?

Le centre des opérations de sécurité (SOC) de GoSecure a plus de 400 000 heures d'expérience dans l'analyse des alertes, la définition de la gravité et l'exécution d'une réponse.

La combinaison de la technologie AV traditionnelle et de la nouvelle génération fournit un flux régulier d'alertes, bien au-delà de la technologie AV traditionnelle seule.

Le SOC de GoSecure rend opérationnelle votre protection NGAV afin d'optimiser ses capacités de sécurité.

[CONTACTEZ-NOUS : +1 (855) 893-5428]

www.gosecure.ai/fr

BLOQUEUR D'EXPLOITATION

Le bloqueur d’exploitation surveille les applications typiquement exploitables (navigateurs, lecteurs de documents, clients de messagerie, Flash, Java et autres). Au lieu de viser des identifiants CVE particuliers, il se concentre sur les techniques d'exploitation. Lorsqu'elle est déclenchée, la menace est immédiatement bloquée sur la machine.

« SANDBOX » INTÉGRÉ AU PRODUIT

Les logiciels malveillants actuels sont souvent fortement masqués et tentent d’échapper autant que possible à la détection. Pour voir à travers cela et identifier le comportement réel caché sous la surface, nous utilisons le sandboxing intégré au produit. En émulant différents composants matériels et logiciels informatiques, le sandboxing peut exécuter un échantillon suspect dans un environnement virtualisé isolé.

PROTECTION CONTRE LES « BOTNETS »

La protection contre les « Botnet » détecte les communications malveillantes utilisées par les réseaux de zombies, tout en identifiant les processus incriminés. Toute communication malveillante détectée est bloquée et signalée à l'utilisateur.

SUPPORT MULTIPLATEFORME

NGAV GoSecure TitanMC prend en charge tous les systèmes d'exploitation, y compris Windows, Mac et Linux.

[CONTACTEZ-NOUS : +1 (855) 893-5428]

GoSecure est un leader et un innovateur reconnu en matière de cybersécurité, pionnier de l'intégration de la détection des menaces au niveau des points d'extrémité, du réseau et de la messagerie électronique en un seul service géré de détection et de réponse étendues (MXDR). La plateforme GoSecure TitanMC offre une détection prédictive multi-vectorielle, une prévention et une réponse pour contrer les cybermenaces modernes. GoSecure TitanMC MXDR offre une réponse rapide et des services d'atténuation active qui touchent directement le réseau et les points de terminaison des clients. Depuis plus de 20 ans, GoSecure aide ses clients à mieux comprendre leurs lacunes en matière de sécurité et à améliorer leurs risques organisationnels et leur maturité en matière de sécurité grâce aux solutions MXDR et aux services professionnels fournis par l'une des équipes les plus fiables et les plus compétentes de l'industrie. Pour en savoir plus, visitez le site :

www.gosecure.ai/fr

Votre allié pour consolider, évoluer et prospérer

GoSecure