

MALWAREBYTES ENDPOINT DETECTION AND RESPONSE

Détection, isolation et remédiation sur Windows et Mac pour les entreprises

PRÉSENTATION GÉNÉRALE

Selon une étude récente du Ponemon Institute, 68% des personnes interrogées ont confié avoir subi une ou plusieurs attaques dommageables sur des terminaux, compromettant des données sensibles ou l'accès à différentes infrastructures. Des études similaires montrent que près de 60% des terminaux hébergent des menaces cachées dont des trojans, rootkits ainsi que des backdoors. Ces menaces sont sophistiquées, persistantes et échappent souvent aux différentes solutions de protection des terminaux, ce qui explique pourquoi plus de la moitié des entreprises signalent une incapacité à détecter et à traiter efficacement les attaques modernes.

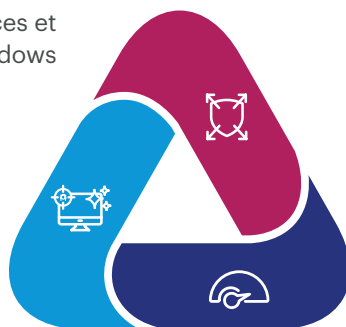
Tout aussi important : les changements récents des mandats de conformité nécessitant une protection plus stricte des données à caractère personnel (DCP). Les directives du New York Department of Financial Services (NYDFS) et du California Consumer Privacy Act (AB 375) font partie des plus rigoureuses, mais la plupart des États américains disposent aujourd'hui de réglementations plus strictes. Si les équipes de sécurité ne peuvent pas prouver que les alertes de « faux positifs » ne sont pas des menaces ou des offensives réelles, leurs entreprises pourraient être verbalisées et obligées de faire des annonces publiques, voir convoquées au tribunal par le procureur général ou d'autres acteurs du service public ou privé. En Europe, les nouvelles réglementations General Data Protection Regulation (GDPR) et Payment Services Directive 2.0 (PSD2) créent par ailleurs des défis certains.

Recherche de menaces et ransomware rollback

Recherche guidée sur les menaces et ransomware rollback pour Windows

Détection, isolation et remédiation aux menaces

Diminuez les risques et les faux positifs ; bloquez les menaces grâce à de multiples modes d'isolation



DÉFIS EDR

Le nombre d'attaques a doublé

Plus de 68% des organisations ont récemment subi une ou plusieurs attaques et 80% d'entre elles étaient causées par des nouvelles menaces de type « zero-day ».

Un taux élevé de faux positifs

Près de 60% des sociétés ont besoin d'une protection contre les zero-day, mais un taux élevé de faux positifs reste pour elles un problème fondamental.

Des solutions complexes

Plus de 61% des sociétés affirment que la complexité des technologies liées à l'EDR et des ressources humaines limitées représentent des défis conséquents.

Source : 2020 EDR Study, Ponemon Institute

Déploiement rapide et gestion facile

Déployez en quelques minutes à peine puis gérez l'EDR depuis une console cloud intuitive

DÉCOUVREZ LES AVANTAGES

Les appareils peuvent rester en ligne grâce à l'EDR opérationnel

Il est impératif que vous puissiez remettre rapidement en ligne les terminaux compromis. Notre produit vous permet d'effectuer les opérations d'isolation, d'investigation et de remédiation, dont celle de ransomware rollback, en quelques clics.

Investigation guidée

Notre outil de traque guidée des menaces fournit des indicateurs de compromission (IOC) classés en fonction de la gravité, pour que vous puissiez évaluer rapidement l'étendue et l'urgence d'une menace.

Isolation granulaire des attaques

Notre produit empêche le déplacement latéral d'une attaque par l'isolation d'un segment du réseau, d'un session d'utilisateur ou de la création d'un processus sur le terminal. Cette fonctionnalité offre une marge de manœuvre appréciable à l'utilisateur, qui peut ainsi fournir la réponse active adaptée tout en minimisant l'impact sur l'utilisateur final.

Remédiation complète

La technologie unique 'Linking Engine' de Malwarebytes cartographie les modifications du système liées au malware, supprime intégralement l'infection et rétablit le bon état des terminaux.

Recherche Flight Recorder

Flight Recorder enregistre au fil du temps les changements et activités au niveau des fichiers, des processus, des domaines de réseau et des adresses IP, sur les postes de travail comme sur les serveurs.

Ransomware Rollback

Malwarebytes place les modifications apportées aux fichiers sur le système dans une mémoire cache locale pendant une période de 72 heures. En un clic, vous pouvez annuler les dommages causés par un ransomware et rétablir la bonne santé et la productivité de l'appareil.

Étendez votre protection contre les menaces

Malwarebytes intègre la protection à la détection pour sécuriser vos terminaux et vous apporter une visibilité et un contrôle complet sur toute la chaîne d'attaque.

Cyberveille globale

La cyberveille fournit des données globales sur l'heuristique comportementale, les IOCs et les techniques d'attaques, ce qui permet d'adapter constamment les moyens de détection et de remédiation pour lutter contre les nouvelles menaces.

Protection des terminaux intégrée

Notre produit intègre des techniques de détection automatisées et adaptables, dont une technologie sandbox, qui apprennent à chaque étape du processus de détection des menaces. Ainsi, vous obtenez un aperçu continu des activités suspectes jusqu'à ce que vous puissiez poser un diagnostic final avec précision.

Surveillance des activités suspectes

« Une aiguille dans une meule de foin » : Malwarebytes surveille les terminaux et crée un ensemble de données dans le cloud, où l'analyse comportementale associée à l'apprentissage machine permettent de trouver les « aiguilles » que sont les IOCs.

Sandbox dans le cloud

Nous appliquons une stratégie de cyberveille puissante à l'analyse profonde des menaces inconnues par notre technologie sandbox dans le cloud. Ainsi, nous améliorons la précision de détection des menaces, et vous fournissons une analyse prête à l'emploi d'IOCs à partir desquels vous pouvez prendre des décisions.



fr.malwarebytes.com



emeamsp@malwarebytes.com

Malwarebytes est une société de cybersécurité bénéficiant de la confiance de millions d'utilisateurs à travers le monde. Malwarebytes protège les particuliers et les entreprises de manière proactive contre les menaces malveillantes qui échappent aux antivirus classiques, y compris les ransomwares. Le produit phare de l'entreprise fait appel à une technologie indépendante des signatures pour détecter et arrêter les cyberattaques avant qu'elles ne causent des dégâts. Pour en savoir plus, rendez-vous sur fr.malwarebytes.com.

Copyright © 2022, Malwarebytes. Tous droits réservés. Malwarebytes et le logo Malwarebytes sont des marques de commerce de Malwarebytes. Les autres noms et marques sont la propriété de leurs détenteurs respectifs. Toutes les descriptions et spécifications du présent document sont susceptibles d'être modifiées sans préavis et sont fournies sans garantie d'aucune sorte.