

Malwarebytes Breach Remediation

Suppression avancée des menaces

CARACTÉRISTIQUES TECHNIQUES

- Suppression avancée des programmes malveillants avec analyse anti-rootkit
- Moteur intelligent d'analyse heuristique et basée sur des définitions
- Recherche et suppression automatisées et à distance des programmes malveillants
- Affichage chronologique des événements indésirables
- Indicateurs de menaces OpenIOC personnalisés (format XML)
- Quatre types d'analyse système (complète, rapide, menaces, répertoire)
- Modes analyse & suppression ou analyse uniquement en option
- Gestion de la mise en quarantaine des menaces détectées
- Sauvegarde centralisée des enregistrements d'événements (format CEF)
- Pas d'utilisation permanente de l'espace sur les terminaux
- Moteur de détection des malwares et adwares spécifique aux Mac
- Plateforme extensible avec options de déploiement flexibles

Aujourd'hui, le personnel de réponse aux incidents est gêné par les systèmes traditionnels de détection des brèches qui produisent des milliers d'alertes par jour, mais qui ne peuvent pas complètement éliminer les malwares pour les empêcher de revenir ou de se propager latéralement. Cette approche réactive nécessite des efforts d'investigation manuelle pour trouver la brèche permettant aux attaques malveillantes de ne pas être détectées pendant 205 à 229 jours* en moyenne. Lorsqu'un malware est découvert sur un ordinateur portable ou un serveur, cela peut prendre six heures à un administrateur informatique pour reformater chaque machine infectée.



Malwarebytes Breach Remediation est une plateforme avancée nouvelle génération de détection des menaces et de remédiation pour les petites, moyennes et grandes entreprises. Avec Malwarebytes Breach Remediation, les organisations peuvent chasser les malwares de manière proactive pour résoudre les incidents à distance, plutôt que de se rendre physiquement sur chaque terminal infecté pour nettoyer ou reformater la machine. Il s'agit d'une plateforme autonome qui s'intègre facilement aux outils existants de gestion et de sécurité de l'entreprise. Malwarebytes Breach Remediation permet de détecter et de supprimer simultanément les malwares, ce qui réduit considérablement le risque de menaces persistantes.

Avantages clés

Suppression totale des programmes malveillants

Il supprime toute trace de l'infection et les artefacts associés, pas seulement le code malveillant original, ou infecteur. Il élimine le risque de récurrence de l'attaque et de mouvements latéraux qui profiteraient des traces laissées par le programme malveillant. Malwarebytes est le leader sur le marché de la suppression des programmes malveillants, il est utilisé par des millions de personnes et approuvé par AV-Test.org.

Réduction drastique des temps d'arrêt

Il vous permet de concentrer vos efforts sur des projets plus rémunérateurs au lieu de passer des heures interminables à résoudre manuellement des problèmes d'infection et à réinitialiser le matériel dans l'ensemble de votre entreprise.

*Présentation du Gartner Security & Risk Management Summit, Defending Endpoints From Persistent Attack, Peter Firstbrook, 8-11 juin 2015.

Institut Ponemon, Étude Cost of Data Breach, juin 2016.



Proactif, pas réactif

Il déploie une suppression automatique qui détecte et résout simultanément de manière proactive les incidents. C'est comme installer un système de pulvérisation pour stopper les petits incendies avant qu'ils ne deviennent incontrôlables. Il fait de vous le héros en vous permettant de résoudre le problème plutôt que de réagir à des milliers d'alertes de sécurité par jour.

La traque des programmes malveillants

Il découvre les programmes et activités malveillants nouveaux et non détectés et les supprime rapidement. Il utilise les règles de comportement et la technologie heuristique de Malwarebytes, en plus des indicateurs de compromission (IOC) d'outils et référentiels tiers de détection des intrusions.

Il extrait les événements indésirables

Il traque les événements indésirables grâce à une fonctionnalité exclusive de chronologie légale afin que votre équipe puisse remédier aux lacunes de sécurité et aux comportements dangereux des utilisateurs. Il rassemble les événements système avant et pendant une infection et présente les données dans une chronologie pratique pour l'analyse complète du vecteur et de la chaîne d'attaque. Les événements couverts incluent les modifications de fichiers et de registres, l'exécution de fichiers et les sites Web visités.

Améliore les investissements existants

Il s'intègre aisément aux outils existants de gestion des informations et des événements (ex. : Splunk, ArcSight, QRadar), les systèmes de détection d'intrusion (ex. : Lastline, Mandiant, Fidelis) et les plateformes de gestion des terminaux (ex. : Tanium, ForeScout, Microsoft SCCM). Vous pouvez lancer le déploiement et activer la suppression des menaces à partir de votre plateforme de gestion des terminaux sur la base d'alertes envoyées par votre SIEM et renvoyer automatiquement des consignes de résolution à votre SIEM.

Comble les lacunes de sécurité d'Apple

Élimine rapidement les malwares et adwares des terminaux Mac. Nettoie les systèmes OS X en moins d'une minute de A à Z. Une interface utilisateur séparée et des programmes de commande en ligne permettent un déploiement flexible avec des solutions de gestion populaires Mac (p. ex. Apple Remote Desktop, Casper Suite, Munki). Permet un fonctionnement à distance automatisé grâce à des commandes shell ou AppleScript. Les administrateurs système et les intervenants en cas d'incidents peuvent collecter des informations système grâce à la commande pratique Snapshot.

CONFIGURATION REQUISE

Rendez-vous sur malwarebytes.com/business/breachremediation pour connaître l'intégralité des spécifications techniques et la configuration requise.

Composants inclus :

Programme CLI Windows
Programme de chronologie légale Windows
Programme GUI Mac
Programme CLI Mac

Terminaux

Systèmes d'exploitation pris en charge :

Windows 10, 8.1, 8, 7, Vista, XP
Windows Server 2012, 2008, 2003
Mac OS X (10.8 et versions supérieures)



malwarebytes.com/business



corporate-sales@malwarebytes.com



1.800.520.2796

Malwarebytes protège les consommateurs et les entreprises contre les menaces dangereuses telles que les malwares, les ransomwares et les exploits qui échappent à la vigilance des solutions antivirus traditionnelles. Malwarebytes Anti-Malware, le produit phare de la société, dispose d'un moteur hautement avancé de détection heuristique des menaces qui a permis l'élimination de plus de cinq milliards de menaces sur les ordinateurs du monde entier. C'est pourquoi plus de 10 000 PME et grandes entreprises du monde entier font confiance à Malwarebytes pour protéger leurs données. Fondée en 2008 et basée en Californie, la société possède des bureaux en Europe et emploie une équipe internationale de chercheurs et d'experts.