FICHE TECHNIQUE

Malwarebytes Endpoint Detection and Response

Fonctionnalités de protection, de détection et de réponse intégrées pour assurer le parfait fonctionnement des appareils.

Présentation

D'un côté, les organisations de toutes tailles sont menacées par des attaques de plus en plus amples et profondes, perpétrées par des malwares toujours plus sophistiqués. De l'autre, elles mettent en place diverses mesures de sécurité, telles qu'antivirus, surveillance des systèmes, etc. Or, les malwares ont appris à dénicher les failles qui existent entre ces systèmes de défense compartimentés.

Malwarebytes Endpoint Detection and Response (EDR) est une suite complète de détection, de protection et de remédiation des malwares qui permet à l'EDR opérationnel d'assurer le bon fonctionnement des appareils. Elle offre une détection étendue sur toute la chaîne d'attaque et permet des opérations rapides et efficaces. Basée sur le cloud et dotée d'une interface unique quelle que soit la taille de votre organisation, Malwarebytes EDR offre une solution de détection sophistiquée capable d'identifier même les exploits zero-day, des capacités d'investigation intuitives ne nécessitant pas un niveau de connaissances inatteignable, et une possibilité de récupération même lorsque le ransomware est déjà déclenché.

POINTS CLÉS

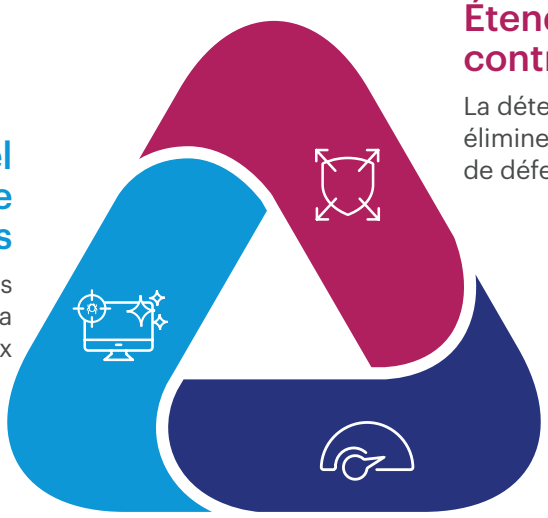
Suite complète
Un système centralisé unique traite tous vos besoins de sécurité opérationnelle des terminaux.

Ransomware Rollback
Fait revenir l'appareil dans un état sain connu, même après le déclenchement du ransomware.

Efficace tout en restant transparent
Optimise l'efficacité des professionnels de la sécurité, tout en étant transparent pour l'utilisateur final.

L'EDR opérationnel assure la bonne marche des appareils

Un objectif unique de maintenir les terminaux en ligne et d'assurer la productivité des utilisateurs finaux



Étendez votre protection contre les menaces

La détection et l'analyse intégrées éliminent le cloisonnement des outils de défense

Déployez rapidement, gérez efficacement

Déployez, gérez et ajustez la sécurité des terminaux avec rapidité et efficacité

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. De plus, nos outils de traque intelligente des menaces vous offrent des options d'analyse, pour mettre en liste blanche les logiciels que vous approuvez et mieux examiner les comportements suspects.

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. La réponse aux incidents intégrée vous permet d'isoler et de remédier toutes les traces d'une menace ou d'exclure les activités que vous jugez sans danger, en quelques clics, sans recours aux scripts. Le maître mot, la flexibilité : les exclusions sont globales ou se font en fonction des stratégies.

Isolation granulaire des attaques
Notre produit empêche le déplacement latéral d'une attaque par l'isolation d'un segment du réseau, d'un appareil ou d'un processus sur l'appareil. 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 propriétaire de Malwarebytes Linking Engine 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 terminaux comme sur les serveurs. L'outil de recherche Flight Recorder permet de traquer les menaces non spécifiques dans toute la flotte d'appareils gérés par Malwarebytes EDR. Elle offre des capacités de recherche avancée de hash MD5, de noms de fichier, de domaines de réseau, d'adresses IP et plus encore. Cette fonctionnalité permet de rechercher des IOC spécifiques pouvant être mappés à des techniques MITRE ATT&CK.

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 complets sur toute la chaîne d'attaque.

Cyberveille globale
La cyberveille fournit des données globales sur l'heuristique comportementale, les IOC et les techniques d'attaque, qui permettent 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 un 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 créé un ensemble de données dans le cloud, où l'analyse comportementale associée à l'apprentissage machine permettent de trouver les « aiguilles » que sont les IOC.

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

Déployez rapidement, gérez efficacement.

Malwarebytes est pensé pour aller vite, du déploiement à la gestion en passant par la maintenance en continu. Les organisations peu dotées en ressources de sécurité parviennent à définir une stratégie de sécurité et à activer leur réponse en quelques minutes.

Recours au cloud lorsque c'est nécessaire
En profitant de la puissance de la plateforme cloud Malwarebytes Nebula, les fonctionnalités de détection et de réponse pour terminaux évoluent à la même vitesse que les innovations des pirates informatiques. En outre, notre agent à faible empreinte se sert de la puissance du cloud pour détecter efficacement les menaces avancées d'après leur comportement.

Gestion pensée pour les terminaux
Notre produit vous permet de gérer efficacement la sécurité des terminaux à l'échelle de l'entreprise et, en quelques clics, de passer d'un tableau de bord global à une menace mise en avant, puis à la remédiation de groupes d'appareils ou d'emplacements en fonction de priorités.

Automatisation des opérations et du suivi
Vous pouvez lancer en quelques clics les tâches de sécurité basiques telles que les analyses et les remédiations. De plus, le suivi est automatisé pour que les terminaux n'ayant pas effectué une analyse ou terminé une remédiation soient marqués à des fins d'action supplémentaire. L'automatisation de ces fonctions vous permet de gagner du temps pour vous consacrer à des tâches de sécurité plus stratégiques.

Avantages

Optimisez la disponibilité des appareils
EDR met à disposition des moyens puissants, de la détection à la récupération d'un appareil sur lequel s'est déclenché un ransomware, pour assurer le fonctionnement continu des appareils.

Traquez les menaces sans connaissances pointues
Malwarebytes met à profit des techniques brevetées et leader sur le marché pour fournir aux professionnels de sécurité une cyberveille globale adaptée à leur environnement et facile à analyser même sans connaissances pointues.

Gérez plus d'appareils avec moins d'efforts
L'automatisation et le suivi des tâches clés, telles que les analyses et les remédiations, permettent aux professionnels de sécurité de gérer un plus grand nombre d'appareils en faisant moins d'efforts.

PLUS D'INFOS

Pour en savoir plus, contactez votre équipe de compte ou votre partenaire de distribution autorisé. Sinon, pour échanger avec un expert commercial près de chez vous, rendez-vous sur : malwarebytes.com/business/contact-us/

malwarebytes.com/business corporate-sales@malwarebytes.com +1 800 520 2796

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 www.malwarebytes.com.