DOSSIER SPÉCIAL

Malwarebytes | DataVenir abonnements – logiciels

MALWAREBYTES ENDPOINT DETECTION AND RESPONSE

Détection, isolation et remédiation de classe professionnelle pour Windows, Mac et Linux

PRÉSENTATION

Dans un rapport d'étude récent du Ponemon Institute , 68 pour cent des participants signalaient une ou plusieurs attaques de terminaux dommageables ayant compromis des informations ou des infrastructures importantes. Une étude similaire montre que près de 60 pour cent des terminaux hébergent des menaces cachées, dont des chevaux de Troie, des rootkits et des backdoors dangereux. Ces menaces sont sophistiquées, persistantes et parviennent à déjouer même les meilleures protections de terminaux, ce qui explique pourquoi plus de la moitié des entreprises déclarent être incapables de détecter et de traiter efficacement les menaces avancées.

De façon tout aussi préoccupante, les changements récents des obligations de conformité exigent une protection plus stricte des informations d'identification personnelle. Les directives du New York Department of Financial Services (NYDFS) et le California Consumer Privacy Act (AB 375) font partie des règlementations les plus contraignantes, mais la plupart des États des États-Unis s'arment désormais de lignes directrices plus strictes encore. Si les équipes de sécurité ne sont pas en mesure de prouver que les faux positifs ne sont pas de réelles menaces ou attaques, les organisations s'exposent à des amendes, des obligations de s'exprimer publiquement et des poursuites judiciaires. En Europe, le RGPD (Règlement général sur la protection des données) et le PSD2 (Deuxième directive sur les services de paiement) engendrent également de nouveaux défis.

Les organisations ont besoin de pouvoir détecter immédiatement les menaces connues et inconnues, d'y répondre activement en temps réel et d'isoler et d'investiguer en profondeur. En cas de perte de données ou de demande de rançon, elles doivent être capables de remédier, de revenir en arrière et de récupérer rapidement et en totalité.

PROBLÉMATIQUES D'EDR

Les attaques ont doublé
Plus de 68 % des entreprises ont récemment fait l'objet d'attaques, dont 80 % étaient de nouvelles menaces zero-day.

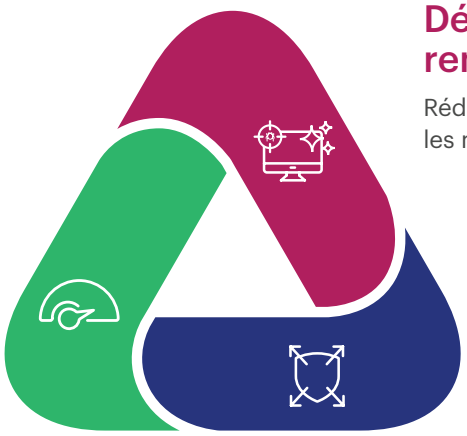
De hauts niveaux de faux positifs
Près de 60 % des entreprises ont besoin d'une détection « zero-day », mais le taux de faux positifs est une préoccupation majeure.

Des solutions complexes
Plus de 61 % des entreprises disent que la complexité et le manque de personnel constituent des problématiques importantes dans le domaine des EDR.

Source : 2020 EDR Study, Ponemon Institute

Déploiement rapide et gestion facile

Déployez la solution en quelques minutes et gérez-la depuis la console intuitive native du cloud



Détection, isolation et remédiation des menaces

Réduisez les risques et les faux positifs ; arrêtez les menaces avec plusieurs modes d'isolation

Traque des menaces et retour en arrière en cas de ransomware

Traquez les menaces et effectuez un ransomware rollback sur Windows de façon guidée

SIMPLE

Malwarebytes Endpoint Detection and Response (EDR) pour Windows, Mac et Linux peut facilement remplacer ou compléter d'autres solutions de sécurité des terminaux, dont Microsoft Defender.Nous avons gagné la fidélité et la reconnaissance de nos clients, car notre solution est souple et directe, et son déploiement via un agent de terminal unique est économique. Elle offre de plus des intégrations intéressantes et une bonne compatibilité.

- Sans perturber vos systèmes, déploiement en quelques minutes
- Un seul agent de terminal, une intégration simple
- Console de gestion intuitive sur le cloud

EFFICACITÉ

Malwarebytes EDR utilise un machine learning de détection des anomalies pour détecter dynamiquement les attaques du Web, les malwares zero-day, les ransomwares, les programmes ou modifications potentiellement indésirables (PUP et PUM) et les infections provenant de dispositifs USB. Malwarebytes EDR est extrêmement précis, ce qui explique pourquoi nous enregistrons l'un des taux de faux positifs les plus bas du secteur. Nos capacités d'isolation ultrapointue empêchent le mouvement latéral d'une attaque en vous permettant de contenir des machines, sous-réseaux ou groupes tout en poursuivant vos activités de réponse active.

- Détection des menaces zero-day avec un faible taux de faux positifs
- Isolation pointue des processus, des réseaux et des ordinateurs Windows
- Suppression des exécutables, des artefacts et des modifications

EFFICIENCE

Malwarebytes EDR offre le retour en arrière en cas de ransomware sur Windows, et pour éviter tout impact sur les performances, utilise un agent léger qui nécessite seulement trois processus d'arrière-plan, soit bien moins que d'autres solutions.

- Agent léger unique, pas d'impact sur les performances
- Ransomware rollback de 72 heures sur Windows
- Faible coût total de propriété

PROTECTION DES TERMINAUX PROACTIVE INTÉGRÉE

Malwarebytes EDR inclut une protection des terminaux intégrée et des techniques de détection adaptatives automatisées qui apprennent à chaque étape du processus de détection des menaces. Contrairement à des solutions basées sur signatures plus réactives, qui laissent les malwares s'exécuter avant d'intervenir, notre protection des terminaux trouve et bloque les menaces avant que les appareils se retrouvent infectés. Malwarebytes EDR reconnaît et bloque dynamiquement et précisément le code malveillant et les comportements suspects.

MODES D'ISOLATION PROPRES AU SYSTÈME D'EXPLOITATION

Malwarebytes EDR est la première solution à fournir plusieurs modes combinés d'isolation des terminaux. En cas d'attaque de terminal, vous pouvez facilement empêcher le malware de se propager et de nuire, et atténuer les perturbations pour les utilisateurs et le système informatique pendant l'attaque.

- **L'isolation des réseaux** Limite les communications entre appareils pour bloquer les cybercriminels et empêcher les malwares d'entrer en contact avec leurs auteurs.
- **L'isolation des processus** restreint les opérations autorisées à s'exécuter afin de freiner les malwares, tout en permettant aux utilisateurs de rester productifs.
- **L'isolation des postes** sur Windows alerte les utilisateurs sur les menaces et bloque temporairement l'accès tout en maintenant l'appareil en ligne à des fins d'analyse.

REMÉDIATION AUTOMATISÉE ET COMPLÈTE

Notre approche automatisée permet aux analystes informatiques et de sécurité d'éliminer les tâches manuelles pour remédier les attaques, leur faisant ainsi gagner un temps précieux. Les infections par malware typiques peuvent laisser derrière elles plus de 100 artefacts, dont des fichiers, des dossiers et des clés de registre capables de se propager à d'autres systèmes au sein du réseau d'une organisation. La plupart des solutions se contentent de remédier les composantes de malware actives, telles que les exécutables, ce qui expose les systèmes à la réinfection.

La technologie propriétaire Linking Engine de Malwarebytes détecte et supprime les artefacts dynamiques et associés, les modifications et les altérations de processus. Notre moteur applique un séquençage associé pour garantir une désinfection complète des mécanismes de persistance des malwares.

SANDBOX DANS LE CLOUD

Pour augmenter la précision de détection des menaces, Malwarebytes utilise un sandbox dans le cloud, c'est-à-dire un bloc virtuel servant à isoler et déclencher les malwares potentiellement nuisibles à des fins d'évaluation et d'analyse.

Le sandbox vous permet d'investiguer le code suspect, même à distance, sans interrompre la productivité des utilisateurs finaux. Après l'analyse, Malwarebytes vous remet un rapport complet pour que vous puissiez répondre de façon appropriée aux indicateurs de compromission (IOC).

TRAQUE GUIDÉE DES MENACES

L'interface de visualisation ergonomique présente un tableau récapitulatif Kanban qui classe automatiquement la combinaison d'actions dans le MITRE ATT&CK Framework , ce qui vous permet de comprendre rapidement pourquoi notre algorithme de machine learning a jugé que l'activité suspecte nécessitait votre attention. Nous fournissons également, à l'attention des analystes forensic qui ont besoin d'une vue détaillée, une chaîne d'actions et de commandes liées pour qu'ils aient à disposition les IOC nécessaires.

De plus, l'interface de visualisation peut être lancée dans la sous-fenêtre de Flight Recorder Search (FRS) sans que vous perdiez l'endroit où vous vous trouvez. FRS est une interface d'utilisateur guidée qui vous aide à rechercher de façon systématique les fils d'Ariane ou indices (indicateurs) sur tous les terminaux gérés de votre entreprise, afin de vous permettre de détecter les premiers signes de mouvement latéral d'une menace.

RANSOMWARE ROLLBACK SUR WINDOWS

Pour les plateformes Windows, Malwarebytes EDR inclut une technologie unique de ransomware rollback de 72 heures capable de retourner en arrière et de faire revenir vos systèmes à leur état d'origine. Si une attaque touche les fichiers d'un utilisateur, Malwarebytes peut facilement annuler ces changements pour restaurer les fichiers chiffrés, supprimés ou modifiés lors d'une attaque de ransomware. Cerise sur le gâteau, notre technologie de stockage de données propriétaire minimise l'espace requis pour sauvegarder vos données.

SURVEILLANCE CONTINUE

La fonctionnalité de recherche Flight Recorder de Malwarebytes EDR fournit une surveillance et une visibilité continues sur Windows et Mac, de façon à obtenir des données utiles. Elle comprend des capacités de recherche de noms de fichier, de domaines réseau, d'adresses IP, de hachages MD5 et de chemins ou noms de processus/fichiers. Vous pouvez également afficher automatiquement les activités suspectes, afficher tous les détails des lignes de commande des processus exécutés et stocker trente jours de données temporaires dans le cloud.

VULNERABILITY ET PATCH MANAGEMENT

Notre module Vulnerability Assessment s'intègre et s'appuie sur les outils de visibilité et de prévention de notre solution EDR pour vous aider à renforcer vos défenses depuis une seule et même plateforme de sécurité cloud. En s'appuyant sur un inventaire à jour de votre logiciel, des pilotes et des systèmes d'exploitation (SE), notre module Vulnerability Assessment identifie les vulnérabilités logicielles connues, qui sont des éléments que les menaces peuvent utiliser pour accéder à votre réseau. Il hiérarchise ensuite les actions recommandées en fonction du niveau de risque présenté par chaque vulnérabilité identifiée. Le module Patch Management de Malwarebytes prend le contrôle du processus de correction du logiciel. Combiné à notre module Vulnerability Assessment, le module Patch Management accélère l'identification, le déploiement, l'installation et la vérification des révisions sur les terminaux Windows et les SE de serveur, ainsi que sur de nombreuses applications tierces.

FILTRAGE DNS

Le module Malwarebytes Domain Name System (DNS) Filtering aide à empêcher les utilisateurs sur site et à distance d'accéder à du contenu web inapproprié ou à des sites web malfaisants, et vous permet de faire appliquer vos codes de conduite d'entreprise. De plus, notre module DNS Filtering chiffre toutes les demandes liées au nom de domaine pour limiter les moyens par lesquels les menaces exploitent les sites et applications web. Pour réduire encore plus les risques, DNS Filtering est complété par la protection en temps réel Malwarebytes contre les téléchargements malveillants.

MANAGED DETECTION AND RESPONSE

Malwarebytes propose également une solution Managed Detection and Response (MDR) pour les entreprises de toutes tailles limitées en termes de ressources de cybersécurité. Avec Malwarebytes MDR , votre environnement est protégé par Malwarebytes EDR, et notre équipe de professionnels en cybersécurité disposant de plusieurs décennies d'expérience surveille votre environnement 24 h/24, 7 j/7 pour investiguer les alertes que Malwarebytes EDR génère en temps réel. De plus, notre équipe Malwarebytes MDR remédie les menaces ou offre des conseils de remédiation à votre équipe, ce qui vous permet de faire gagner du temps à vos ressources en informatique et en sécurité, leur permettant de se consacrer à d'autres projets plus urgents.

HAUT RETOUR SUR INVESTISSEMENT FAIBLE COÛT TOTAL DE PROPRIÉTÉ

Avec notre solution native cloud, Malwarebytes EDR évolue facilement pour répondre à tous vos besoins futurs. Notre expertise de cyberintelligence en remédiation vous offre une solution alimentée par le renseignement sur des menaces provenant de millions de terminaux protégés par Malwarebytes, chez des particuliers comme dans des entreprises. L'API Malwarebytes facilite l'intégration à SIEM, SOAR, ITSM, etc., pour aller encore plus loin dans l'automatisation et la compatibilité. Malwarebytes EDR garantit un haut retour sur investissement et un faible coût total de propriété, et nous sommes également réputés pour notre service et notre assistance de qualité.

VOTRE CHOIX LE PLUS SÛR EN MATIÈRE D'EDR

La solution Malwarebytes de classe professionnelle Endpoint Detection and Response pour les plateformes Windows, Mac et Linux détecte les activités suspectes, isole les attaques, investigue les menaces et remédie les dommages de façon efficace et efficiente.

Les autres solutions peuvent être difficiles à déployer et à gérer, et ne sont généralement pas compatibles avec d'autres logiciels de sécurité comme Microsoft Defender. La plupart des autres solutions EDR suppriment uniquement les exécutables et n'offrent pas de multiples couches d'isolation pour arrêter les menaces avant qu'elles puissent nuire. Elles sont également conçues pour donner l'alerte à chaque menace, ce qui explique leur taux élevé de faux positifs.

Malwarebytes EDR s'intègre facilement et est compatible avec la plupart des autres solutions de sécurité des terminaux, y compris Microsoft Defender. Avec un déploiement et une gestion simples par l'intermédiaire de notre console cloud Nebula, nous détectons efficacement les activités suspectes et isolons les processus et les réseaux pour réduire les dommages. L'isolation des bureaux est également disponible sur les postes de travail Windows. La technologie propriétaire Malwarebytes Linking Engine supprime les artefacts, les modifications et les altérations de processus tout en fournissant un ransomware rollback unique de 72 h sur les postes Windows. Malwarebytes EDR pour Windows, Mac et Linux utilise un agent léger unique sans impact sur les performances.

N'attendez pas qu'il soit trop tard. Malwarebytes représente votre choix le plus sûr pour l'EDR sur Windows, Mac et Linux. Nous avons gagné la reconnaissance et la fidélité de nos clients pour notre EDR de classe professionnelle simple, efficace et efficient.

NOUS CONTACTER

DataVeniR
abonnements – logiciels

www.datavenir.com

04.58.57.08.85

malwarebytes.com/business

mbpartner@malwarebytes.com

Malwarebytes considère que lorsque les personnes et les entreprises ne se sentent pas menacées, elles peuvent prospérer. Ne proposant pas simplement la remédiation des malwares, l'entreprise fournit des solutions de cyberprotection, de protection de la vie privée et de prévention à des dizaines de milliers de consommateurs et d'entreprises chaque jour. Pour en savoir plus, rendez-vous sur https://www.malwarebytes.com.