FICHE TECHNIQUE

Malwarebytes **Endpoint Protection & Response**

Remédier aux incidents au-delà de la simple alerte

La dure vérité, c'est qu'à l'heure actuelle aucun produit de cybersécurité ne protège à 100 % contre toutes les menaces : www.malwarebytes.com/remediationmap.

Contre des intrusions inévitables, la remédiation est essentielle.

Les organisations sont aujourd'hui à la recherche de solutions capables de résoudre les incidents contre lesquels leurs défenses actuelles sont inefficaces. Une attaque qui a réussi à contourner ces défenses peut rester indétectée pendant des semaines voire des mois. En 2017, une étude mondiale du Ponemon Institute a montré que le temps moyen nécessaire à l'identification d'une intrusion est de 191 jours.

Les solutions englobant Endpoint Detection and Response (EDR) visent à accélérer la détection des menaces pour réduire leur temps de présence. Plus vite une violation de données sera identifiée et contenue, moins son coût sera élevé pour l'organisation. Les solutions EDR actuelles identifient les menaces qui ont réussi à contourner les protections traditionnelles et interviennent en général sous la forme de journaux, d'alertes et d'e-mails de notification. Un analyste expert en menaces déploie alors des outils pour étudier le code, puis les machines infectées sont réimagées.

Malwarebytes Endpoint Protection and Response diffère dans sa démarche. Malwarebytes déploie la remédiation Linking Engine ainsi que Ransomware Rollback, des technologies propriétaires qui vont au-delà des alertes et du réimageage pour réparer les dommages causés par une intrusion. Avec Endpoint Protection and Response, plus besoin d'accepter le compromis entre coût et complexité.

CARACTÉRISTIQUES TECHNIQUES

Protection Web
Empêche l'accès aux sites Web malveillants, réseaux publicitaires, réseaux criminels et « bas-fonds » du Web.

Sécurisation renforcée des applications
Réduit la surface de vulnérabilité aux exploits et détecte de façon proactive les tentatives de collecte d'empreintes des attaques avancées.

Réduction des risques liés aux exploits
Détecte et bloque de façon proactive les tentatives d'abus de vulnérabilité et d'exécution de code à distance sur le terminal.

Protection contre les comportements d'application
Empêche l'exploitation des applications dans le but d'infecter le terminal.

Apprentissage automatique appliqué à la détection des anomalies
Permet l'identification proactive des virus et des malwares grâce à des techniques d'apprentissage automatique.

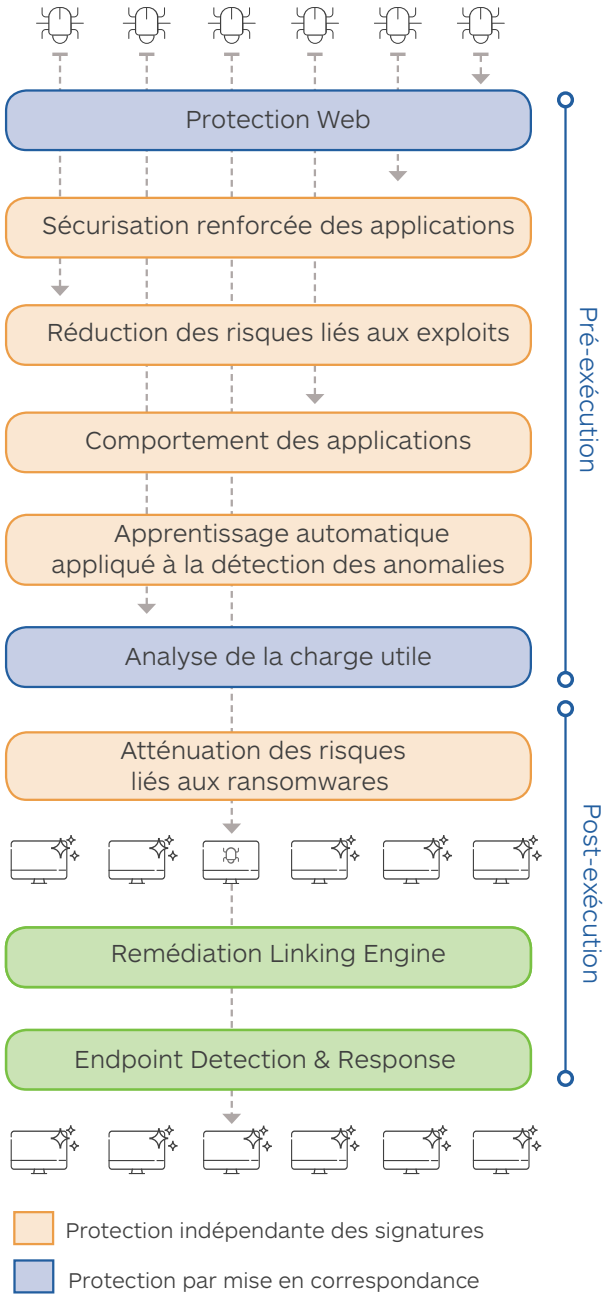
Analyse de la charge utile
Fait appel à des règles heuristiques et comportementales pour identifier des familles entières de malwares connus et pertinents.

Atténuation des risques liés aux ransomwares
Détecte et bloque les ransomwares grâce à une technologie de surveillance des comportements.

Linking Engine et remédiation
Remédie complètement les infections dans leur globalité avec un impact minimal sur l'utilisateur final. Votre terminal est de nouveau en parfaite santé.

Endpoint Detection and Response (EDR)
Surveille les terminaux en continu à des fins d'analyse comportementale et d'investigation. Réduit le temps de présence des menaces zero day. Permet d'intervenir au-delà de la simple émission d'une alerte.

ENDPOINT PROTECTION & RESPONSE



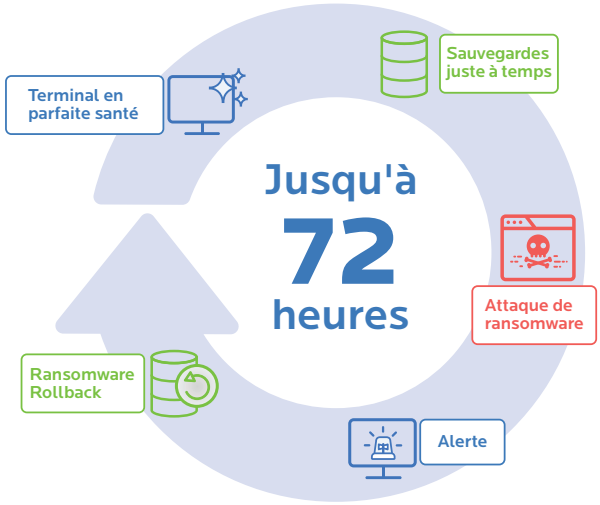
Avantages clés

Protection multicouche
La protection multivecteur (MVP) de Malwarebytes déploie une approche multicouche incluant des techniques de détection statiques et dynamiques pour assurer une protection à toutes les étapes d'une attaque. Vos terminaux sont protégés contre tous les types de menaces, des virus classiques aux menaces avancées de demain.

Visibilité des terminaux pour une surveillance en continu
L'enregistreur de vol Flight Recorder assure une surveillance et une visibilité en continu des postes de travail MS Windows pour maximiser les informations à votre disposition. Vous pouvez facilement suivre l'activité du système de fichiers, du réseau, des processus et du registre. Les événements Flight Recorder sont stockés localement et dans le cloud.

Trois modes d'isolation des terminaux
Lorsqu'un terminal est infecté, Malwarebytes l'isole pour stopper l'hémorragie. Des capacités de remédiation rapides empêchent le déplacement latéral de l'infection. Les malwares ne peuvent pas contacter leurs auteurs et les cybercriminels qui attaquent à distance sont alors bloqués. Endpoint Protection and Response est le premier produit qui offre trois modes d'isolation d'un terminal : l'isolation du réseau restreint les communications entre les différents processus ; l'isolation des processus restreint l'exécution de ceux-ci ; enfin, l'isolation du terminal alerte l'utilisateur final et empêche les interactions. Le système reste en ligne de manière sécurisée pour permettre son analyse en profondeur.

Remédiation complète globale
Malwarebytes offre les capacités de remédiation les plus fiables du marché. C'est pour cela que chaque jour nos produits sont téléchargés 500 000 fois et remédient 3 millions d'infections dans le monde entier. Malwarebytes Endpoint Protection and Response déploie notre technologie propriétaire Linking Engine afin d'éliminer toute trace de l'infection ainsi que ses artefacts, et plus seulement la charge utile de la menace primaire. Cette approche réduit le temps habituellement consacré à formater et à réimager les terminaux.



Ransomware Rollback
La technologie Ransomware Rollback permet de retourner en arrière pour annuler les effets d'un ransomware en déployant des sauvegardes réalisées juste à temps. Malwarebytes enregistre et associe les modifications à des processus spécifiques. Chaque modification effectuée par un processus est enregistrée. Si un processus exécute une « mauvaise » action, vous pouvez facilement annuler les modifications associées et restaurer les fichiers qui ont été cryptés, supprimés ou modifiés. Pour limiter les données stockées, notre technologie propriétaire d'exclusion dynamique apprend à reconnaître les actions des « bonnes » applications.

Gestion centralisée dans le cloud
La gestion centralisée dans le cloud simplifie le déploiement et la prise en main, peu importe le nombre de terminaux. Elle vous évite en outre d'avoir à maintenir une solution matérielle sur site.

malwarebytes.com/business | corporate-sales@malwarebytes.com | 1.800.520.2796

Malwarebytes est une entreprise 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.