

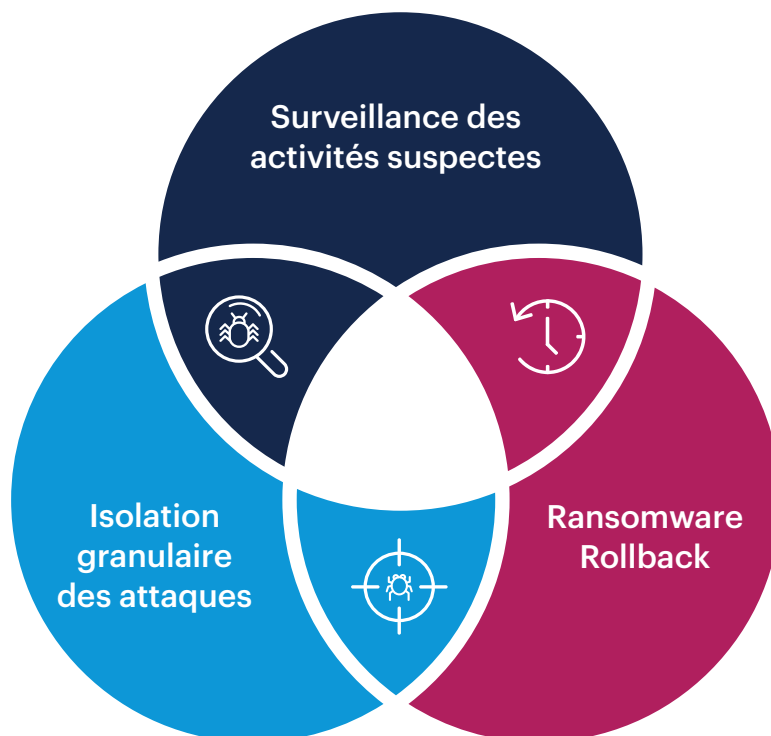
Malwarebytes Endpoint Detection and Response for Servers

Protection, détection et réponse intégrées. Rapidité et simplicité d'utilisation.

Présentation

Les serveurs professionnels et les données qu'ils contiennent représentent le nerf de la guerre dans les opérations des entreprises modernes. Une cyberattaque réussie peut anéantir un système essentiel pour une société et anéantir sa productivité. On le sait, les serveurs sont au cœur de toute l'activité d'une organisation, et c'est pour cela qu'ils méritent d'être totalement sécurisés de façon à pouvoir résister à n'importe quelle attaque.

Malwarebytes Endpoint Detection and Response for Servers constitue une solution rapide, légère et spécifiquement conçue pour les serveurs en vue de protéger vos données les plus précieuses. Cette solution associe protection proactive intégrée et remédiation rapide et permanente pour que votre infrastructure de serveurs reste en ligne et opérationnelle. De plus, avec la fonctionnalité Ransomware Rollback, vous pouvez rétablir le parfait état des serveurs touchés sans passer par un réimageage coûteux, ni craindre pour votre productivité ou payer une rançon.



AVANTAGES CLÉS

Visibilité complète

Une gestion dans le cloud centralisée qui offre une visibilité complète sur votre stratégie de sécurité.

Efficacité

Une détection continue des menaces de sécurité avancées et une réponse adaptée, pour une efficacité opérationnelle inégalée.

Précision du diagnostic

Une détection intégrée de toute la chaîne d'attaque qui permet de rendre un diagnostic précis.

Adaptabilité à vos plateformes

Malwarebytes offre une protection avancée qui correspond aux besoins de la plateforme de votre organisation, depuis les serveurs jusqu'aux postes de travail.

PLATEFORMES

Serveurs Windows

Fonctionnalités

Déployez rapidement. Gérez simplement.

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 rapidement à une réponse active et une stratégie de sécurité efficace.

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, le recours à la puissance du cloud, qui diminue l'empreinte sur les serveurs, permet de détecter efficacement les menaces avancées d'après leur comportement.

Gestion pensée pour les terminaux

Notre solution vous permet de gérer efficacement la sécurité des serveurs à l'échelle d'une entreprise. En quelques clics, vous disposez d'une large visibilité depuis le tableau de bord général jusqu'aux indicateurs de compromission (IOC) découverts sur un serveur.

Étendez votre protection contre les menaces.

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

Protection proactive intégrée

La fonction automatisée de détection et de protection contre les menaces sur le Web, dans les mémoires, les applications et les fichiers applique des techniques de détection adaptables, comme la surveillance des comportements et l'apprentissage machine basé sur le cloud.

Surveillance des activités suspectes

Analyse en continu les processus des terminaux, les registres, les systèmes de fichiers et l'activité réseau dans le cloud à l'aide de l'analyse comportementale et de l'apprentissage machine pour repérer les activités potentiellement suspectes.

Sandbox dans le cloud

L'analyse profonde des menaces inconnues est effectuée en toute sécurité dans le cloud. Grâce à la cyberveille, une détection ultraprécise est obtenue, ainsi que des IOC sur lesquels se baser pour prendre des décisions.

Recherche Flight Recorder

L'outil Flight Recorder enregistre au fil du temps les changements au niveau des fichiers, des processus, des domaines de réseau et des adresses IP. Il traque ainsi les menaces non spécifiques pour obtenir des IOC tels que des hash MD5, des noms de fichier, des domaines de réseau et des adresses IP.

Investiguer, isoler et récupérer.

Malwarebytes Endpoint Detection and Response for Servers offre aux professionnels de la sécurité la capacité d'investiguer rapidement, d'isoler et d'éliminer en profondeur les menaces et d'effectuer une récupération en quelques minutes.

Isolation granulaire des attaques

Vous pouvez désormais empêcher facilement les malwares de se propager en cas d'attaque de serveur. Malwarebytes Endpoint Detection and Response for Servers exploite tout le potentiel des capacités de réponse informatique en se basant sur trois modes d'isolation des appareils :

1. L'isolation du réseau limite les possibilités de communication des appareils, bloquant ainsi les attaques et empêchant les malwares de contacter leurs auteurs. Elle restreint aussi le déplacement latéral des malwares.
2. L'isolation des processus empêche les malwares d'engendrer de nouveaux processus et limite ainsi leur impact. Pour ne pas compliquer le travail de réponse, le lancement de nouvelles applications par les utilisateurs est interdit.
3. L'isolation des serveurs permet aux administrateurs de bloquer l'accès à une machine pendant que l'équipe informatique effectue le triage. Elle peut aussi être utilisée pour prévenir les menaces provenant de l'intérieur.

Grâce aux différents modes d'isolation des serveurs, les équipes de sécurité peuvent prendre des mesures concrètes pour répondre aux menaces.

Remédiation complète

Solution rapide et permanente, la remédiation Malwarebytes vous aide à supprimer définitivement tous les malwares. Les approches traditionnelles consistent à supprimer uniquement les fichiers exécutables actifs en ignorant les modifications résiduelles, qui entraînent des réinfections.

La technologie propriétaire Linking Engine de Malwarebytes surveille les artefacts, les changements, les altérations de processus, y compris les fichiers exécutables de mémoire laissés de côté par les autres solutions.

Ransomware Rollback

Notre technologie Ransomware Rollback agit de concert avec la surveillance des activités suspectes pour détecter les comportements de ransomwares. Si un comportement suspect est détecté, Malwarebytes active le processus de récupération des fichiers en chiffrant et en déplaçant les données pour pouvoir les restaurer plus tard.

Le processus de récupération des fichiers limite la sauvegarde au chiffrement juste à temps des fichiers. En un clic, les équipes de réponse aux incidents peuvent annuler les dommages causés par les ransomwares en rétablissant l'état précédant l'attaque des fichiers affectés, jusqu'à 72 heures avant leur compromission.

Avantages

Protection complète pour vos actifs les plus précieux

Assurez la protection avancée innovante des actifs importants de votre organisation. Avec la surveillance des activités suspectes, l'isolation granulaire des attaques et la fonctionnalité Ransomware Rollback, les organisations peuvent garantir la bonne marche de leurs systèmes, même dans le cas d'une cyberattaque d'ampleur.

Sécurité des serveurs discrète et sur mesure

Malwarebytes Endpoint Detection and Response for Servers offre l'équilibre parfait entre protection et performances. Déployez rapidement la protection des terminaux pour vos serveurs sans affecter la puissance de traitement du système.

Visibilité ultraprécise depuis une console cloud centralisée

Notre console cloud centrale offre une visibilité complète sur votre stratégie de sécurité. Via un écran unique doté d'une UI intuitive, gagnez en visibilité sur toute l'activité de votre organisation, des serveurs aux postes de travail.

Résumé

Les serveurs d'entreprise sont constamment à la merci des attaques. Pour fournir les services, les applications et les autres ressources essentielles à la bonne tenue des opérations, les serveurs ont besoin de ce qui se fait de meilleur en matière de protection.

De la protection à la détection et à la réponse, Malwarebytes Endpoint Detection and Response for Servers protège les données les plus sensibles des organisations. Pensé pour les organisations de toute taille dont l'efficacité est au cœur des préoccupations, Malwarebytes Endpoint Detection and Response for Servers est entièrement conçu pour s'intégrer et communiquer avec la chaîne de détection, à partir d'un agent unique et d'une console de gestion, pour permettre aux organisations de gérer la sécurité des serveurs rapidement, facilement et en s'adaptant à leur environnement.

DEMANDER UN ESSAI

Pour demander un essai gratuit,
rendez-vous sur : malwarebytes.com/business/request_trial



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.

© Malwarebytes 2020. 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.