Fiche produit

Bitdefender
BUILT FOR RESILIENCE

GravityZone Security EDR Cloud

Détection et réponse avancées pour les endpoints (EDR)

Les cybercriminels ne cessent de s'améliorer et les attaques avancées sont de plus en plus difficiles à détecter. En utilisant des techniques qui, prises en considération de manière isolée peuvent ressembler à des comportements normaux, un attaquant peut accéder à votre infrastructure en restant invisible pendant des mois, augmentant ainsi significativement les risques de coûteuses violations de données. Lorsque votre solution de sécurité pour endpoints ne vous fournit pas le degré de détection et les mécanismes de réponse dont vous avez besoin pour faire face aux attaques avancées, l'ajout de GravityZone EDR Cloud, facile à utiliser, renforce rapidement et efficacement vos opérations de sécurité.

GravityZone EDR Cloud surveille votre réseau pour détecter de manière précoce les activités suspectes et vous fournit les outils dont vous avez besoin pour contrer les cyberattaques. Le Machine Learning éprouvé de Bitdefender et l'analyse dans le cloud et en sandbox permettent de détecter les activités qui échappent aux mécanismes de prévention traditionnels. La solution fournit une visibilité complète sur les techniques, tactiques et procédures (TTP) utilisées lors des attaques et propose un système de recherche complet pour les indicateurs de compromission (IoC), les techniques MITRE ATT&CK, ainsi que d'autres artefacts pour détecter rapidement les attaques.

GravityZone EDR Cloud fournit des visualisations innovantes et faciles à comprendre, avec un contexte et des renseignements sur les menaces étoffés qui aident le personnel informatique à comprendre les chemins d'attaque et à identifier les lacunes en matière de protection. Ces visualisations simplifient l'investigation et la réponse, allégeant les tâches pesant sur le personnel informatique. L'analyse en sandbox permet d'exécuter automatiquement les charges utiles suspectes dans un environnement virtuel clos afin d'isoler et de neutraliser les fichiers douteux. Les fonctionnalités de GravityZone EDR Cloud protègent les entreprises des menaces avancées tout en permettant une chasse aux menaces proactive et l'analyse des causes racines.

Comment GravityZone EDR Cloud peut vous aider ?

- **En détectant et en répondant de manière avancée aux attaques.** En surveillant votre réseau pour détecter rapidement les activités suspectes et fournir les outils dont vous avez besoin pour y faire face.
- **En comblant votre manque de personnel et/ou de compétences en sécurité.** En permettant à vos équipes de répondre efficacement, avec une priorisation automatique des alertes et des mesures applicables en un clic.
- **En réduisant votre risque organisationnel.** En analysant en continu votre infrastructure pour identifier les risques sur la base de centaines de facteurs. En vous aidant à atténuer les risques liés aux utilisateurs, aux réseaux et aux systèmes d'exploitation.
- **En minimisant votre charge opérationnelle.** Fournis dans le cloud et ne nécessitant que peu de maintenance, les agents sont faciles à déployer et à intégrer à votre architecture de sécurité existante. Ils sont également entièrement compatibles avec votre solution antimalware pour endpoints.

Une innovation pour une efficacité et une efficience améliorées

La technologie de corrélation multi-endpoints de Bitdefender révolutionne la détection et la visibilité sur les menaces grâce à l'application de capacités

En bref

GravityZone EDR Cloud détecte en temps réel les menaces avancées, dont les attaques sans fichier, les ransomwares et menaces Zero day. Le collecteur d'évènements dans le cloud surveille en continu les endpoints et priorise les évènements de sécurité dans une liste pour l'investigation et la réponse. L'EDR fournit des visualisations innovantes et faciles à comprendre, avec un contexte et des renseignements sur les menaces qui aident à comprendre les chemins d'attaque et à identifier les lacunes de sécurité. Ces visualisations simplifient l'investigation et la réponse, allégeant les tâches pesant sur le personnel informatique.

Avantages clés

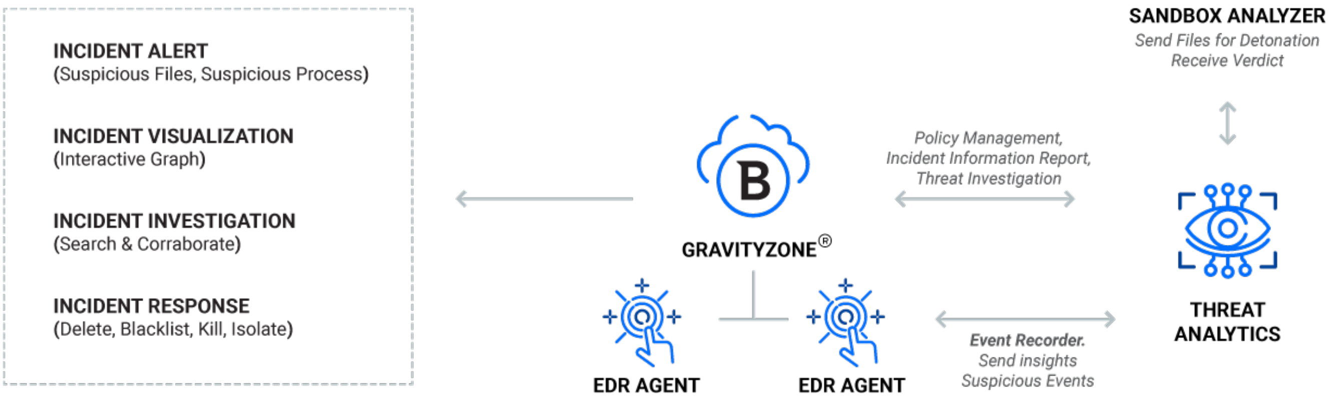
- Détection à la pointe de l'industrie associée à une visibilité sur les attaques permettant d'activer le plein potentiel de la technologie XDR. Des capacités de recherche complètes pour des indicateurs de compromission (IoC), des techniques MITRE ATT&CK et d'autres outils pour la découverte d'attaques en amont.
- Investigation et réponse ciblées : la visualisation des événements au niveau de l'entreprise permet de répondre de manière efficace, tout en limitant les déplacements latéraux et en bloquant les attaques en cours.
- Efficacité maximale : notre agent facile à déployer et peu coûteux garantit une efficacité et une protection maximales, avec un minimum d'efforts. Pour bénéficier d'une solution managée, vous pouvez évoluer vers Bitdefender MDR (Managed Detection and Response).

« Les capacités EDR de GravityZone donnent des informations détaillées sur le fonctionnement des incidents et leurs effets tout au long de la chaîne d'attaque. Cela nous fait gagner un temps considérable en matière d'enquête, puisque le travail manuel est éliminé. »

Sascha Neuhaus,
IT Security Officer, Louis

XDR permettant de révéler les attaques avancées sur les nombreux endpoints présents dans les infrastructures hybrides (postes de travail, serveurs ou conteneurs fonctionnant sous différents systèmes d'exploitation). La solution étend les capacités de l'EDR en matière de visibilité, d'analyse et de corrélation des événements, hors des limites d'un endpoint isolé, pour permettre aux équipes de sécurité de traiter plus efficacement les cyberattaques complexes impliquant plusieurs endpoints. La technologie de corrélation entre les endpoints combine la granularité et le riche contexte de sécurité offerts par l'EDR avec les systèmes d'analyse à l'échelle de l'infrastructure du XDR (eXtended Detection and Response). En permettant la visualisation des menaces au niveau de toute l'entreprise, l'XDR vous aide à cibler vos investigations et à réagir de manière plus efficace.

Comment cela fonctionne



GravityZone EDR Cloud est une solution basée dans le cloud et intégrée à la plateforme Bitdefender GravityZone XDR. Chaque agent EDR déployé sur les endpoints de votre organisation possède un enregistreur d'évènements qui surveille en continu l'endpoint et envoie, de manière sécurisée, des renseignements et des informations sur les évènements suspects à la console centralisée de GravityZone (Control Center). Dans le Control Center, le moteur de corrélation entre les endpoints de Bitdefender collecte les évènements relatifs aux appareils et les distille en des vues priorisées des incidents de sécurité de toute l'entreprise, permettant ainsi aux administrateurs de rapidement examiner les menaces et d'appliquer efficacement les mesures nécessaires.

Bitdefender
BUILT FOR RESILIENCE

49 rue de la vanne

92120 Montrouge

France

Bitdefender est un leader mondial de la cybersécurité qui fournit des solutions de pointe en matière de prévention, de détection et de réponse aux menaces. Protégeant des millions d'environnements de particuliers, d'entreprises et de gouvernements, Bitdefender compte parmi les experts les plus fiables de l'industrie pour l'élimination des menaces, la protection de la vie privée et des données, et la cyber-résilience. Grâce à des investissements importants dans la recherche et le développement, les Bitdefender Labs découvrent plus de 400 nouvelles menaces chaque minute et répondent à environ 40 milliards de requêtes de menaces par jour. La société a été la première à innover dans le domaine des malwares, de la sécurité de l'IoT, de l'analyse comportementale et de l'intelligence artificielle. Sa technologie est utilisée sous licence par plus de 150 éditeurs parmi les plus reconnus au monde. Fondée en 2001, Bitdefender a des clients dans 170 pays et possède des bureaux dans le monde entier.

Pour plus d'informations, rendez-vous sur : https://www.bitdefender.fr.

Bitdefender-BSG-GZ-EDRCloud-Datasheet-DEX4610-fr_FR
CD-Apr/10/2022 • MD-Apr/10/2022