FICHE PRODUIT

Utilisation Web uniquement

Bitdefender

Solution de détection et de réponse dédiée aux endpoints (EDR)

Détection des menaces avancées, investigation ciblée et réponse efficace

www.bitdefender.fr

Défis posés par les menaces avancées

Les cybercriminels ne cessent de s'améliorer et les attaques avancées d'aujourd'hui 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.

Que fournit Bitdefender Endpoint Detection and Response (EDR) ?

Lorsque votre solution de sécurité pour endpoints ne fournit pas la visibilité et les mécanismes de réponse dont vous avez besoin, l'ajout de Bitdefender Endpoint Detection and Response (EDR) permet d'améliorer rapidement et efficacement vos opérations de sécurité, notamment par sa simplicité.

Détection et réponse des attaques avancées

Bitdefender EDR surveille votre réseau pour détecter rapidement les activités suspectes et vous fournit les outils dont vous avez besoin pour répliquer.

- L'EDR intègre le Machine Learning primé de Bitdefender, l'analyse dans le cloud et en sandbox pour détecter les activités passant outre les mécanismes de prévention traditionnels pour les endpoints.
- Une visibilité complète sur les techniques, tactiques et procédures (TTP) utilisées pour attaquer vos systèmes.
- Des fonctionnalités de recherche d'indicateurs de compromission (IoC) spécifiques, des techniques MITRE ATT&CK et d'autres outils pour détecter très rapidement les attaques. Dans l'évaluation MITRE ATT&CK réalisée en avril 2020, Bitdefender a excellé en matière de détections et d'alertes exploitables, et ce à toutes les étapes de la chaîne d'attaque
- Prenez des mesures de réponse pour corriger les vulnérabilités et éliminer les risques d'attaques récurrentes.

Comble les lacunes en compétences de cybersécurité

- Des flux de travail simples à suivre et intégrés en matière de réponse permettent à votre équipe de réagir efficacement, de limiter les déplacements latéraux et de bloquer les attaques en cours.
- La visualisation des menaces vous aide dans vos investigations en vous permettant de comprendre les détections complexes, à identifier la cause racine des attaques et à maximiser votre capacité à réagir directement.
- Priorisation automatique des alertes avec fonctionnalités de résolution en un clic.

Réduit le risque organisationnel

- L'EDR analyse en continu la sécurité de votre entreprise en identifiant les risques selon des centaines de facteurs. Il donne des indications claires pour vous aider à limiter les risques liés à vos utilisateurs, vos réseaux et vos systèmes d'exploitation.

Minimise la charge opérationnelle

- Basé dans le cloud et ne nécessitant que peu de maintenance, l'EDR Bitdefender est facile à déployer et à intégrer à votre architecture de sécurité existante. Il est également entièrement compatible avec votre solution antimalware pour endpoints.
- Un agent léger qui prend peu d'espace disque, de mémoire, de bande passante et de ressources du processeur.
- Flexible, évolutif et pouvant être mis à jour vers la plateforme de protection complète pour endpoints de Bitdefender et vers une solution MDR (Managed Detection and Response).

Fonctionnement de la solution

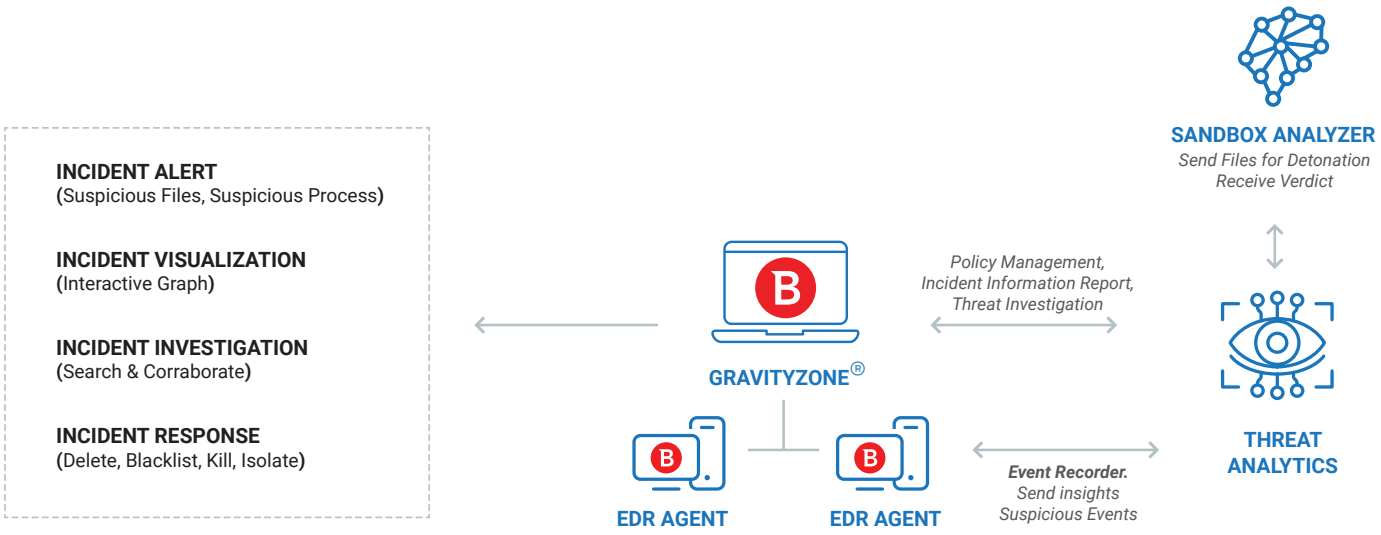

Schéma de Bitdefender Endpoint Detection and Response

Bitdefender EDR est une solution fournie dans le cloud et intégrée à la plateforme Bitdefender GravityZone. Des agents EDR sont déployés sur vos endpoints. Chaque agent EDR dispose d'un enregistreur d'événements qui surveille en continu l'endpoint et envoie en toute sécurité des informations et événements suspects au cloud de GravityZone.

Le module Threat Analytics collecte et regroupe les événements des endpoints au sein d'une liste priorisée d'incidents pour permettre l'investigation et la réponse. Il envoie les fichiers suspects à Sandbox Analyzer pour détection puis utilise le verdict de celui-ci dans les rapports d'incident de l'EDR. Le tableau de bord en temps réel est accessible depuis n'importe quel appareil pour permettre aux administrateurs de visualiser les alertes, d'enquêter et de réagir de manière efficace en cas de menace.

Fonctionnalités de Bitdefender Endpoint Detection and Response

Analyse des risques

Analyse des risques humains et de l'endpoint
Analyse en continu les risques de votre entreprise en utilisant des centaines de facteurs pour identifier, prioriser et fournir des instructions visant à limiter les risques liés aux utilisateurs, aux réseaux et aux endpoints.

Détection

Technologie de détection des menaces à la pointe de l'industrie
Détecte les menaces avancées, y compris les attaques sans fichiers, les ransomwares et autres menaces de type Zero-day en temps réel. Complète la solution de sécurité actuelle de vos endpoints pour renforcer la détection.

Analyse sur les menaces
Un collecteur d'événement dans le cloud regroupe en permanence les événements des endpoints dans une liste priorisée d'incidents pour permettre l'investigation et la réponse.

Enregistreur d'évènements
Surveillance en continu des événements de l'endpoint pour permettre la visualisation des actions impliquées lors d'une attaque.

Sandbox Analyzer
Exécute automatiquement les charges actives suspectes dans un environnement virtuel confiné. Le module d'analyse des menaces utilise ensuite cette analyse pour prendre des décisions en ce qui concerne les fichiers suspects.

Investigation et réponse

Recherche d'IoC
Envoie des requêtes à la base de données des événements pour détecter les menaces. Détecte les techniques MITRE ATT&CK et les indicateurs de compromission. Informations en moins d'une minute sur les menaces et autres malwares pouvant être impliqués.

Visualisation
Guides visuels faciles à configurer, enrichis de contextes et de Threat Intelligence, affichant les chemins d'attaque critiques pour soulager les tâches du personnel IT. Aide à identifier les lacunes de protection et l'impact d'un incident à des fins de conformité.

Exécution
Les investigations en sandbox à la demande vous aident à prendre des décisions éclairées sur les fichiers suspects.

Liste des fichiers bloqués
Bloque la propagation des fichiers ou processus suspects détectés par l'EDR sur d'autres machines.

Arrêt des processus
Stoppe instantanément les processus suspects pour bloquer les violations potentielles.

Isolement du réseau
Bloque les connexions entrantes et sortantes d'un endpoint pour empêcher les déplacements latéraux et les autres violations pendant que l'enquête sur l'incident est en cours.

Remote Shell
Exécution de commandes à distance sur n'importe quel poste de travail pour réagir immédiatement aux incidents en cours.

Rapports et alertes

Tableaux de bord et rapports
Tableaux de bord configurables et capacités de reporting en temps réel ou programmé.

Notifications
Tableaux de bord configurables et notifications par e-mail.

Intégration SIEM et prise en charge d'API
Prend en charge l'intégration à des outils tiers.

Performance et administration

Agent EDR optimisé
Faible consommation du processeur, de la RAM et de l'espace disque.

Console Web
Administration simple, dans le cloud.

POURQUOI CHOISIR BITDEFENDER ?

LEADER INCONTESTÉ EN MATIÈRE D'INNOVATION

38% des éditeurs de solutions de cybersécurité au niveau mondial intègrent des technologies Bitdefender. Une présence dans plus de 150 pays.

LA PREMIÈRE SOLUTION COMPLÈTE DE LUTTE CONTRE LES VIOLATIONS

Première plateforme de sécurité intégrant renforcement, prévention, détection et réponse pour les endpoints, les réseaux et le cloud.

LEADER MONDIAL EN CYBERSÉCURITÉ. RÉCOMPENSÉ PAR DE NOMBREUX PRIX.

AV comparatives CERTIFIED ATP Enterprise 2019

AV comparatives Product of the Year 2019

FORRESTER WAVE LEADER 2019 Cloud Workload Security

BITDEFENDER GravityZone Elite v6.6.2.166 ADVANCED ENDPOINT PROTECTION NSS RECOMMENDED

Bitdefender

Création en 2001, Roumanie
Nombre d'employés : plus de 1800

Siège
Enterprise HQ - Santa Clara, CA, États-Unis
Technology HQ - Bucarest, Roumanie

BUREAUX DANS LE MONDE
USA & Canada : Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe : Copenhague, DANEMARK | Paris, FRANCE | Munich, ALLEMAGNE | Milan, ITALIE | Bucarest, Iasi, Cluj, Timisoara, ROUMANIE | Barcelone, ESPAGNE | Dubai, UAE | Londres, ROYAUME-UNI | La Haye, PAYS-BAS
Australie : Sydney, Melbourne

SOUS LE SIGNE DU LOUP

La sécurité des données est un domaine où seuls l'ingéniosité, la vision la plus claire, l'esprit le plus vif et la plus grande perspicacité permettent de gagner dans un contexte qui ne tolère aucune erreur. Notre travail consiste à gagner mille fois sur mille, un million de fois sur un million, et à chaque fois que nécessaire.

Et c'est ce que nous faisons. Nous surpassons les standards de l'industrie, non seulement parce que nous avons la vision la plus claire, l'esprit le plus vif et la meilleure perspicacité, mais aussi parce que nous avons une longueur d'avance sur tous les autres acteurs, qu'il s'agisse des cybercriminels ou de nos confrères experts en cybersécurité. Nous puisons dans le **loup-dragon**, symbole des guerriers roumains au temps des Daces, son intuition, sa force, son agilité et sa clairvoyance, pour vous prémunir contre tous les dangers cachés dans les arcanes du monde numérique.

Nous sommes le loup-dragon et nous utilisons son super pouvoir au cœur de tous nos produits et solutions qui changent la donne.

Bitdefender-EDR-DS-WebUseOnly-creat4933-fr_FR
11/19/20November 19, 2020 9:28 pm11/19/20