Bitdefender Endpoint Detection and Response (EDR)

Aperçu de la solution

Les cybercriminels utilisent des techniques qui, individuellement, ressemblent à des comportements normaux. Un attaquant peut accéder à une infrastructure et rester invisible pendant des mois, ce qui augmente considérablement le risque d'une violation de données. Lorsque la sécurité des endpoints ne fournit pas la visibilité et la réponse nécessaires face aux attaques, l'ajout d'un outil EDR, renforce rapidement et efficacement les opérations de sécurité.

DÉTECTION

- Leader en Machine Learning, en analyses dans le cloud et en sandbox
- Visibilité complète sur les techniques, tactiques et procédures (TTPs)
- Capacités de recherche complètes pour les IoC et les techniques MITRE ATT&CK

INVESTGATION & RÉPONSE

- Flux de travail permettant de limiter la propagation et de stopper les attaques
- Visualisation des menaces pour comprendre les détections et identifier les causes racines
- Alertes hiérarchisées avec résolution en un clic

EFFICACITÉ

- Agent facile à déployer, administré depuis le cloud
- Analyse des risques des utilisateurs et des endpoints
- Flexible et évolutif vers les solutions complètes EPP et MDR de Bitdefender

Bénéfices clés de la solution

Capacités	Description / Capacités
Analyse des risques des endpoints et des utilisateurs	Contrairement à d'autres solutions EDR, Bitdefender analyse en continu l'infrastructure en utilisant des capacités uniques pour identifier les risques sur la base de centaines de facteurs. Elle fournit des conseils clairs pour aider à atténuer les risques liés aux utilisateurs, au réseau et aux systèmes d'exploitation.
Livraison dans le cloud, légèreté et faible maintenance	Fourni dans le cloud et nécessitant peu de maintenance, l'EDR est facile à déployer et à intégrer dans l'architecture de sécurité existante et est entièrement compatible avec toute solution EPP. Son agent léger nécessite peu d'espace disque, de mémoire, de bande passante et de ressources CPU.
Détection des attaques avancées	L'EDR intègre du Machine Learning éprouvé, de l'analyse dans le cloud et en sandbox pour détecter les activités qui échappent aux mécanismes de prévention traditionnels.
Visibilité complète sur les techniques, tactiques et	Des capacités de recherche complètes pour des indicateurs de compromission spécifiques (IoC), des techniques MITRE ATT&CK et d'autres outils permettant de découvrir des attaques en phase initiale. Lors de l'évaluation MITRE ATT&CK d'avril 2020, Bitdefender a excellé dans la

Options de Bitdefender EDR

FONCTIONNALITÉS ET MODULES	BITDEFENDER EDR	EPP + EDR GRAVITYZONE ULTRA	MDR ADVANCED
Antimalware	Rapport uniquement	X	X
Ransomware Prevention & Mitigation	Rapport uniquement	X	X
Windows, MacOS, Linux	Windows uniquement	X	X
Endpoints physiques & virtuels	X	X	X
Agent « léger »	X	X	X
Console d'administration cloud	X	X	X
Remédiation automatique		X	X
Contrôle des apps et des appareils		X	X
Pare-feu sur l'hôte & contrôle Web		X	X
Analyses des risques des apps & appareils	X	X	X
Analyse de la chaîne d'attaque	X	X	X
Full Disk Encryption (add-on)		X	X
Patch Management (add-on)		X	X
Analyse des risques humains	X	X	X
Endpoint Detection and Response (EDR)	X	X	X
Network Traffic Security Analytics (add-on)		X	X

Différenciateurs

- La solution EDR autonome qui inclut l'analyse des risques liés aux utilisateurs
- Un agent EDR léger, à faible consommation de ressources, qui complète toute solution EPP
- Des technologies de prévention de pointe récompensée par les organismes tiers depuis de nombreuses années
- Une Threat Intelligence mondiale basée sur plus de 500 millions de capteurs
- La possibilité de mise à niveau vers le service MDR et les solutions complètes EPP Bitdefender

Bitdefender Endpoint Detection and Response (EDR)

Principaux cas d'utilisation

Situation	Cas d'utilisation	Résultats
Besoin d'un EDR flexible et évolutif	Solution actuelle EPP qui manque d'options pour ajouter un EDR cloud	Ajout facile d'un EDR léger aux solutions EPP concurrentes. Aucune infrastructure de gestion sur site n'est requise
Sopper les attaques avancées	Impossible d'assurer une protection à 100% contre les attaques avancées et persistantes	Détection des activités qui échappent aux mécanismes de prévention EPP
Manque de personnel en cybersécurité	Pas de renseignements et de conseils exploitables sur la manière de traiter les infractions	Intégration facile des flux de travail permettant aux équipes de réponse aux incidents de stopper les attaques et de limiter leur propagation
Réduire le risque	Aucun conseil sur la manière d'améliorer la posture de sécurité	Identification des risques liés aux réseaux, aux applications et aux OS

Profil client type

Typologie	Profil
Taille de l'entreprise	• Entreprises de taille moyenne ayant des besoins de sécurité élevés : 100-1 000 employés (Finance, Santé, Retail, Tech.) • Entreprises du Mid-Market : 1 000 à 10 000 employés
Contact	• RSSI, DSI, Directeur InfoSec/SOC, Responsable Informatique
Profil	• Entreprises avec un SOC • Entreprises avec une équipe InfoSec/IT
Industrie	• Toutes
Exposition aux risques	• Victimes d'APT ou de failles • Prospects sans EDR • Prospects d'industries à risque • Entreprises qui ont des clients ou des partenaires exigeant des mesures de sécurité importantes

Questions de qualification

Besoin d'un EDR flexible et évolutif	1. Avez-vous une solution EDR ? Une solution de ce type pourrait-elle vous aider ? 2. Sous quelle forme préférez-vous que l'EDR vous soit fourni : sur site ou dans le cloud ? 3. A quel point est-ce important que votre nouvel agent EDR soit le plus léger possible ?
Sopper les attaques avancées	1. Comment détectez vous les indicateurs de compromission ou les techniques MITRE ? 2. Comment réagissez vous face à des vulnérabilités et comment éliminez-vous le risque de nouvelles attaques ? 3. Comment bloquez-vous les processus ou isolez-vous un endpoint ?
Manque de personnel en cybersécurité	1. Comment évaluez-vous les connaissances de votre équipe en matière de cybersécurité ? 2. Comment votre équipe détermine-t-elle la cause racine d'une attaque ? 3. À quel point pensez-vous que la visualisation graphique d'une attaque peut vous aider ?
Réduire le risque	1. Comment évaluer où se situent les risques liés aux utilisateurs, aux OS, aux applications et aux réseaux dans votre environnement ? 2. Comment hiérarchiser les tâches nécessaires pour atténuer efficacement ces risques ? 3. En quoi des orientations claires sur l'atténuation de ces risques vous seraient utiles ?

Panorama concurrentiel

Citères d'évaluation	Bitdefender	Sophos	Microsoft	SentinelOne
Analyse des risques des utilisateurs	x		x	
Sandbox Analyzer	x	x		
Visuaisation des menaces	x	x	x	x
Taggage MITRE ATT&CK	x		x	x

Réponses aux objections

Objection	Réponse
Ma solution pour endpoints existante n'offre-t-elle pas ces fonctionnalités ?	Bien que la sécurité des endpoints assure une protection efficace contre de nombreuses menaces, elle ne peut pas assurer une protection totale contre les attaquants avancés qui tentent délibérément de pénétrer dans vos systèmes.
Ne serait-il pas préférable que j'achète l'EDR auprès de mon fournisseur actuel ?	Cela vaut la peine d'y réfléchir, mais Bitdefender EDR peut améliorer votre sécurité en parallèle de votre solution existante. Vous pouvez même migrer plus tard vers la solution complète EPP de Bitdefender.
Je comprends l'intérêt de l'EDR mais mon équipe n'a pas le temps de s'en occuper	Dans ce cas, pourquoi ne pas laisser Bitdefender s'occuper de l'EDR à votre place ? Notre service de détection et de réponse managé est parfait pour les entreprises qui n'ont pas le personnel nécessaire.
Mon entreprise n'est pas assez importante pour que des hackers la ciblent	La plupart des cyberattaques visent les petites entreprises. Votre entreprise possède des données importantes et peut également être une voie d'accès à un client, un partenaire ou un fournisseur.