Fiche produit

ThreatDown Endpoint Detection & Response (EDR)

Prévention, détection et remédiation simples et efficaces

VUE D'ENSEMBLE

Les organisations sont aujourd'hui confrontées à une triste réalité : la perspective d'une cyberattaque n'est plus une question de **"si"**, mais de **"quand"**. Cette réalité est aggravée **par le manque de ressources humaines** en termes de professionnels de la cybersécurité, notamment pour les TPE / PME, ce qui laisse les équipes de **sécurité à court de personnel, pressées par le temps** et confrontées à une **disparité de niveaux de compétences.**

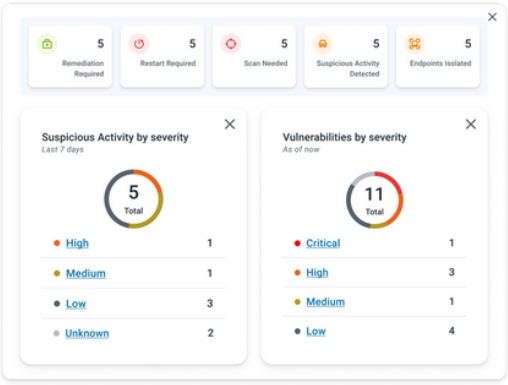
IPgarde tient compte de ce triste constat, et c'est pour cela que nous proposons la solution EDR ThreatDown. Il offre une protection efficace, de **la prévention à la détection** en passant par les actions de **remédiation**. Le gros bonus ? Les utilisateurs ayant une connaissance limitée de la cybersécurité peuvent **facilement apprendre à l'utiliser**. Mais cette simplicité n'enlève rien à sa sophistication sous-jacente : ThreatDown EDR comprend **des outils puissants et des options personnalisables** que les utilisateurs peuvent adopter au fur et à mesure que leur niveau de compétence augmente **et que les besoins de sécurité de l'entreprise évoluent**. En déployant cette plateforme de sécurité basée sur le cloud et facilement accessible, les entreprises de toutes tailles **bénéficient d'une détection et d'une remédiation puissantes,** tout en permettant à leurs équipes de sécurité de **se consacrer à d'autres projets plus urgents.**

DÉFIS

- **Les attaques évoluent** : Plus de 40% des TPE / PME ont connu une cyberattaque avérée en 2023
- **Complexité due à la prolifération des agents** : 55 outils de cybersécurité sont déployés en moyenne dans une entreprise[1]
- **Manque de budget et de ressources :** 80 % des alertes de sécurité sont ignorées par manque de ressources[2]

1 Anomali's Cybersecurity Insights Report 2021 (Rapport sur la cybersécurité 2021).
2 ThreatDown Research

AVANTAGES DE L'EDR THREATDOWN



FACILITÉ D'UTILISATION

ThreatDown EDR offre aux entreprises l'assurance **d'une protection puissante et d'une gestion sans faille.** Facile à apprendre et à utiliser, notre console native s'ouvre sur un tableau de bord intuitif affichant **des repères visuels qui indiquent immédiatement quels sont les points d'extrémité et les serveurs qui nécessitent une attention particulière et pourquoi.**

UNE HAUTE QUALITÉ DE DÉTECTION DES ALERTES SILENCIEUSES

L'EDR émet des alertes avec des aperçus. Les menaces détectées déclenchent des alertes qui contiennent **des informations avec un niveau élevé de détails contextuels** pour aider les utilisateurs **à prendre rapidement des décisions éclairées** sur la façon de réagir.

REMÉDIATION ÉTENDUE

En quelques clics depuis la console de gestion Nebula basée sur le cloud, vous pouvez **remédier à distance à un point de terminaison infecté.** Le moteur de liaison exclusif est conçu pour **identifier et supprimer les artefacts résiduels liés aux logiciels malveillants** et **les changements induits par l'infection** afin de garantir une remédiation complète.

DÉPLOIEMENT ACCÉLÉRÉ

ThreatDown EDR a été conçu en gardant à l'esprit **la facilité d'utilisation et l'accélération du déploiement.** Notre agent léger pour Windows, macOS et Linux **se déploie en quelques minutes.**

EXTENSION DE LA PLATEFORME

ThreatDown EDR s'adapte à l'évolution de vos besoins en matière de sécurité. L'EDR est un composant clé de nos offres groupées qui permettent à votre équipe **de renforcer la prévention dans les principaux vecteurs de menaces** tels que les **vulnérabilités logicielles,** la **gestion des correctifs** et le **filtrage DNS**.

COMMENT CELA FONCTIONNE-T-IL ?

ThreatDown EDR **permet d'empêcher les cybermenaces,** notamment les **malwares**, les **attaques par force brute et les exploits de type " zero-day "**, d'atteindre votre environnement. Pour ce faire, il recherche en permanence les logiciels malveillants connus à l'aide **d'une détection des menaces basée sur des règles**, tout en recherchant de manière proactive les logiciels malveillants inconnus à l'aide **d'une détection basée sur l'IA** (également appelée " basée sur le comportement "). Celle-ci est conçue pour détecter et analyser les fichiers et les programmes anormaux afin **de réduire les risques**. Qu'elles soient connues ou inconnues, les menaces détectées **déclenchent des alertes qui incluent les détails** dont les utilisateurs ont besoin pour **réagir rapidement et de manière appropriée.**

ThreatDown EDR détecte **également les programmes potentiellement indésirables** (PUP) et **les modifications potentiellement indésirables** (PUM) qui, même s'ils ne sont pas malveillants, nuisent souvent à l'expérience des utilisateurs finaux. Il les alerte et les supprime automatiquement. La plateforme évaluée par MITRE automatise également **l'analyse des menaces de type " zero-day "** et permet aux utilisateurs d'isoler le code suspect **par machine, utilisateur et/ou processus** ; le fait de contenir le code douteux permet **d'enquêter sans risque d'exposition et de propagation.** ThreatDown EDR comprend une sandbox dans le cloud que les utilisateurs peuvent utiliser **pour enquêter sur des binaires exécutables douteux** ; les utilisateurs peuvent également utiliser la sandbox pour faire exploser des logiciels malveillants **à distance et en toute sécurité.**

MAINTENIR LE NIVEAU DE MENACE À UN NIVEAU BAS

Protégez les postes de travail, les serveurs et bien plus encore de votre entreprise grâce à des solutions primées de prévention, de détection et de réponse.

- **Détecter avec précision** : Identifier les menaces malveillantes et suspectes.
- **Réagir immédiatement :** Isoler les utilisateurs, les terminaux et les réseaux pour stopper les violations.
- **Remédiation complète** : Remettre les points de terminaison en bon état et prévenir les réinfections.

Lorsque des infections s'infiltrent dans votre environnement numérique, **la détection et la remédiation primées de ThreatDown** peuvent vous aider à **éliminer efficacement les logiciels malveillants.** La technologie de remédiation avancée est conçue pour garantir **l'éradication de toutes les traces résiduelles de logiciels malveillants et l'annulation de toutes les modifications de configuration induites par les logiciels malveillants.** Pour une récupération complète des ransomwares, ThreatDown EDR est fourni avec un Rollback Ransomware de 7 jours (**pour Windows uniquement**) ; cette capacité vous aide à revenir à l'état antérieur au **ransomware sans la tâche fastidieuse de réimager les machines ou de recréer les fichiers cryptés.**

RÉCOMPENSES DE L'INDUSTRIE

La solution ThreatDown est efficace et facile à utiliser. Elle est régulièrement classée au premier rang des certifications de niveau 1 dans les tests à 360° de MRG Effitas et au premier rang des suites de sécurité des points d'extrémité par G2.

MRG Effitas CERTIFIED 360° ASSESSMENT

MRG Effitas CERTIFIED RANSOMWARE

PRENDRE RDV AVEC UN REPRÉSENTANT IPGARDE POUR BÉNÉFICIER DE LA SOLUTION D'EDR THREATDOWN BY MALWAREBYTES

Blog IPgarde
www.blog.ipgarde.com

IPgarde
01 77 49 24 50
contact@ipgarde.com
www.ipgarde.com