

Bitdefender®

MDR

Bitdefender Managed Detection & Response Service

**AMÉLIOREZ VOTRE PROTECTION GRÂCE À NOTRE
SERVICE INFOGÉRÉ DE DÉTECTION ET DE RÉPONSE
(MDR)**

www.bitdefender.fr



Avec des environnements technologiques de plus en plus complexes et en constante évolution, de nombreuses entreprises ont besoin de services pour mieux protéger leurs activités contre des attaques toujours plus sophistiquées. Pour les aider, Bitdefender a lancé un service infogéré de détection et de réponse aux menaces, qui associe nos moteurs de détection et de prévention à une équipe de sécurité disponible 24 h/24 et 7 j/7.

Les entreprises face aux défis de sécurité modernes

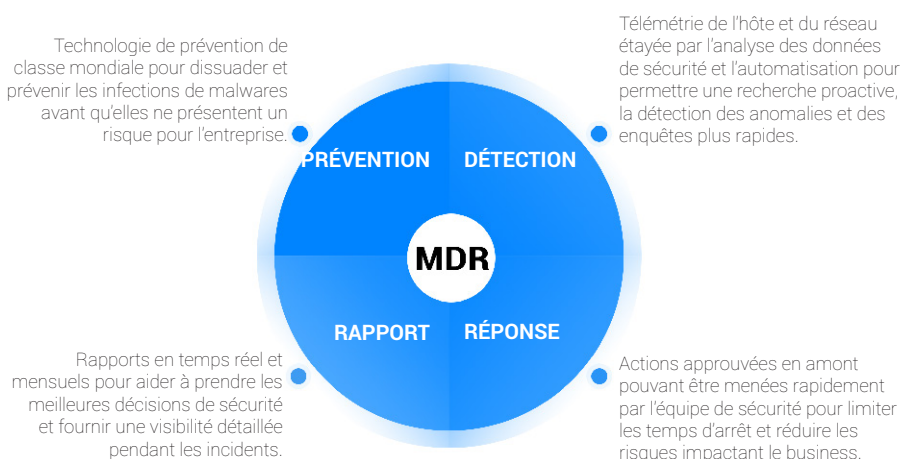
Devant l'ampleur des risques, les entreprises du monde entier accordent de plus en plus d'importance à la cybersécurité. Alors que les attaques gagnent en sophistication et résistent aux méthodes traditionnelles de prévention, les entreprises doivent adapter leur stratégie de sécurité et leurs ressources de manière à repérer efficacement les failles de sécurité et à y répondre rapidement. Selon une enquête menée en 2019 par Accenture sur le coût de la cybercriminalité, les dépenses moyennes des entreprises consacrées à la gestion des incidents de cybersécurité ont augmenté de 72% ces cinq dernières années (pour atteindre les 13 millions de dollars), et le nombre de violations de données a grimpé de 67% au cours de la même période.

D'après le Data Breach Investigations Report (DBIR) réalisé par Verizon en 2019, les ordinateurs portables et de bureau représentaient environ 25% des actifs touchés par des violations de données. Les utilisateurs de ces appareils sont les cibles directes de hackers qui utilisent des techniques d'attaque reposant sur l'ingénierie sociale, comme le phishing. Ce type d'attaque représente environ 33% des cas de violations (soit une progression de 18 points par rapport à 2017). Ainsi, il est indispensable que les services de détection et de réponse soient axés sur les employés et leurs appareils personnels, qui sont souvent le point de départ de la chaîne de compromission.

Les entreprises prennent peu à peu conscience de l'importance de la cybersécurité pour leur business et de la vulnérabilité de leurs systèmes, mais la plupart n'ont pas les ressources suffisantes pour déployer des outils et des process capables de détecter les menaces les plus sophistiquées et d'y répondre efficacement. Cette enquête de Verizon montre aussi que 56% des violations ont été détectées seulement plusieurs mois après l'attaque, alors que les cybercriminels n'ont besoin que de quelques jours, voire minutes, pour compromettre des systèmes et s'en exfiltrer.

Comment le service Bitdefender Managed Detection & Response vient-il en aide aux entreprises ?

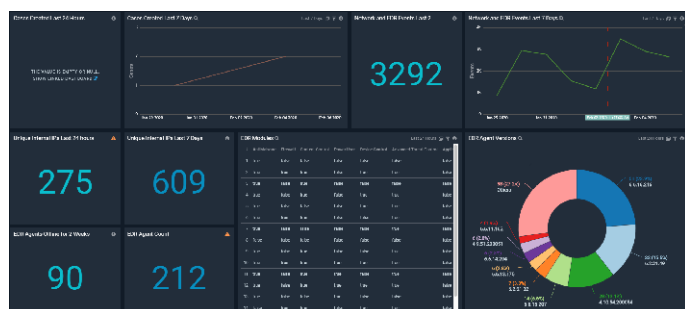
Bitdefender Managed Detection & Response repose sur notre plateforme technologique de nombreuses fois primée, qui agit sur trois niveaux : les endpoints, les réseaux et les analyses de sécurité. Pour obtenir une visibilité totale sur les réseaux et les endpoints, nous combinons la plateforme de protection GravityZone Ultra et la solution Bitdefender Network Traffic Security Analytics. Les données ainsi récoltées alimentent en continu notre plateforme d'analyse de sécurité.



Cette télémétrie permet ensuite de générer des alertes reposant sur la détection directe d'outils, le Machine Learning et le chasse aux menaces. En s'appuyant sur une Threat Intelligence tactique et stratégique, notre chasse aux menaces proactive génère des "missions de repérage" pour nos analystes, visant à détecter les menaces sophistiquées ou les attaquants furtifs qui auraient pu échapper aux outils déjà déployés.

Notre équipe de sécurité étudie tous les incidents détectés par nos outils ou au cours de ses missions de repérage, et y répond en mettant en œuvre une série d'actions préalablement approuvées. Ces actions sont précisées et approuvées par votre équipe IT lors de la mise en place de nos solutions, pour que vous puissiez les exécuter rapidement et bloquer une menace avant qu'elle ne puisse agir.

Les utilisateurs ont des informations en temps réel sur le déroulement des opérations de sécurité, des rapports de synthèse récapitulant les données et les tendances, et des comptes rendus détaillant les circonstances des incidents et les actions mises en œuvre pour éliminer les menaces.



FONCTIONNALITÉS ET AVANTAGES

Détection/prévention sur les endpoints

Technologies de nombreuses fois récompensée, qui bloque les menaces connues et fournit aux analystes des données permettant d'identifier les attaques sophistiquées et les menaces inconnues

Threat Intelligence

Permet de mieux comprendre les cyber risques et de définir des missions de chasse aux menaces

Analyse du trafic réseau

Contrôle des réseaux et des appareils non couverts par la solution de protection des endpoints (IoT, imprimantes, BYOD, etc.)

Actions préalablement approuvées

Isolement et élimination des menaces en temps réel pour limiter le temps de détection et leur diffusion

Gestion technique du compte

Responsable technique de compte fournissant un accompagnement dédié et des bilans trimestriels

Analyse des malwares

Analyses automatiques et à la demande des fichiers susceptibles d'être des malwares

N'hésitez pas à contacter Bitdefender dès aujourd'hui pour en savoir plus sur notre service infogéré de détection et de réponse aux menaces.

Pour plus d'informations, rendez-vous sur www.bitdefender.com/managed-services

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.



Bitdefender

SOUS LE SIGNE DU LOUP

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

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.