- FICHE PRODUIT

Bitdefender

MDR

Bitdefender Managed Detection & Response Service

DES SERVICES MDR MODERNES POUR LES ENTREPRISES DE TOUTES TAILLES

www.bitdefender.fr

Nous exécutons en continu des mesures avancées de prévention et de remédiation des cyberattaques pour que vous n'ayez pas à vous en soucier.

« Bitdefender MDR me permet d'être certain que quelqu'un surveille l'intégralité de notre réseau en temps réel, y compris lorsque mes employés et moi-même ne sommes pas au bureau. » - Directeur Informatique, Archidiocèse

Résoudre les problèmes de cybersécurité des entreprises

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.

> 33% des violations de données sont le résultat d'attaques de type social engineering, comme le phishing. Les ordinateurs portables et les ordinateurs de bureau représentent environ 25% des éléments ciblés par les violations de données – Enquête 2019 DBIR Verizon

Pénurie de personnel : les analystes spécialistes de la sécurité informatique étant rares, leur recrutement est souvent coûteux et difficile. En outre, une enquête récente menée par Ponemon a montré que 60% des employés travaillant dans des SOC avaient déjà pensé à changer de métier à cause du stress.

Détection avancée des attaques : les attaques sophistiquées sont difficiles à détecter car elles utilisent des tactiques, des techniques et des procédures (TTP) qui, individuellement, semblent tout à fait normales. Le budget moyen consacré par les entreprises à la gestion des incidents informatiques a augmenté de 72% ces cinq dernières années. Il s'établit aujourd'hui à 13 millions de dollars. - Enquête 2019 d'Accenture sur le coût de la cybercriminalité.

Investigations longues : les analystes n'ont pas le temps de confirmer toutes les alertes, de les étudier et de définir des priorités pour la suite des enquêtes. Pour la plupart des entreprises, le temps moyen de réparation (MTTR) se compte en mois, alors qu'il faut seulement quelques jours aux attaquants pour compromettre les systèmes et en extraire des données.

Trop d'outils : les entreprises utilisent de multiples consoles et des technologies diverses et variées pour gérer leur infrastructure de sécurité. Près de 40% des personnes interrogées dans le cadre de l'enquête menée par Ponemon ont reconnu qu'elles utilisaient trop d'outils. Et elles sont 71% à souhaiter davantage de solutions automatisées pour la gestion des alertes et le recueil des preuves.

Comment le service Bitdefender MDR vient-il en aide aux entreprises ?

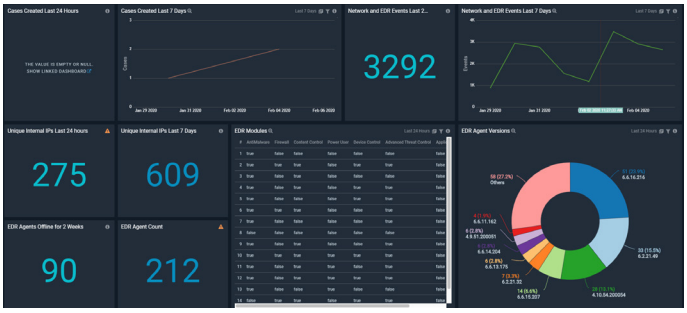
Notre service MDR repose sur l'association de solutions de sécurité de pointe pour les endpoints, de capacités d'analyse de la sécurité du réseau et d'une grande expertise en matière de détection des menaces. Le SOC Bitdefender regroupe des experts ayant travaillé pour les services de sécurité de l'armée de l'US Air Force, de la Navy, de la NSA et des services de renseignements britanniques. Notre méthodologie, inspirée des pratiques militaires, nous a permis de définir des indicateurs pour les attaques nouvelles et sophistiquées et de déployer les contre-mesures appropriées

pour le compte de nos clients.

Personnel du SOC à la demande : Bitdefender met à la disposition de ses clients le personnel d'un centre opérationnel qui s'adapte à leur croissance. Nos analystes suivent les formations nécessaires et maîtrisent les technologies utiles pour les différents environnements qu'ils prennent en charge.

Détection des attaques avancées : nos analystes effectuent des recherches sur les menaces et mettent au point des missions de repérage ciblées en fonction du profil de chaque client, 24h/24, 7j/7 et 365 jours par an. Les données ainsi obtenues s'accompagnent d'informations télémétriques concernant les hôtes et les réseaux, ainsi que d'analyses de sécurité permettant de détecter les attaques avancées et ciblées.

Amélioration de la détection et accélération de la réponse : la télémétrie, les alertes en temps réel provenant de multiples flux de données et les actions en cas d'incident sont adaptées à chaque client pour être plus efficaces, plus rapides et pour limiter les répercussions des incidents sur l'activité.



Réduction de la charge opérationnelle : le service MDR gère vos technologies de sécurité, pour que votre équipe puisse se concentrer sur d'autres projets stratégiques. Cela permet de limiter directement les coûts liés au personnel et à l'acquisition de licences pour les différents outils. Des tableaux de bord actualisé en temps réel, des rapports instantanés et des bilans des actions menées fournissent en continu aux responsables de la cybersécurité un aperçu de la situation de l'entreprise, et des rapports mensuels facilitent la prise de décisions stratégiques.

Options des services Bitdefender MDR

Nous proposons deux packs de services MDR. En fonction du pack choisi, des modules complémentaires sont également disponibles.

	MDR Advanced	MDR Enterprise
Antivirus Next-Gen (NGAV)	✓	✓
Remédiation automatique	✓	✓
Contrôle des applications & des appareils	✓	✓
Pare-feu au niveau de l'hote & contrôle Web	✓	✓
Endpoint Detection & Response (EDR)	✓	✓
Gestionnaire de compte dédié	✓	✓
Analyse des risques liés aux utilisateurs	✓	✓
Chasse aux menaces ciblée	✓	✓
Réponse personnalisée aux incidents	✓	✓
Modélisation des menaces spécifiques à chaque client	✓	✓
Surveillance de l'enregistrement de domaines de phishing		✓
Lutte contre la publication non autorisée de code ou surveillance des informations du client		✓
Surveillance du Dark Web		✓
Intégration avec les outils personnalisés		✓
Surveillance de cibles à grande valeur et à haut risque		✓
Add-Ons		
Protection des appareils IOT sans agent	✓	✓

Pour en savoir plus, rendez-vous sur www.bitdefender.fr/MDR

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

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-MOH-Datasheet-cpad4741-en_FR
03/10/21March 10, 2021 2:37 pm03/10/21