BlackBerry Cybersecurity

GUIDE D'ACHAT

Comment choisir une

SOLUTION DE DÉTECTION ET DE RÉPONSE MANAGÉES (MDR)

AU SOMMAIRE DE CE GUIDE :

- Avantages d'une solution MDR
- Principaux facteurs à prendre en compte lors de la recherche d'une solution MDR
- Création d'un SOC ou achat d'une solution MDR
- Clés pour choisir la solution MDR la mieux adaptée à vos besoins

MDR 24/7

LA CYBERCRIMINALITÉ EST EN HAUSSE ET LES COÛTS À L'ÉCHELLE MONDIALE DEVRAIENT ATTEINDRE 10 500 MILLIARDS DE DOLLARS D'ICI FIN 2025.[1]

Marqué par l'apparition de nouvelles menaces toujours plus sophistiquées chaque mois, voire chaque semaine, le paysage des cybermenaces est en constante mutation. Les ransomwares et les violations de données sont omniprésents, tandis que l'intelligence artificielle se transforme en un outil clé que les cybermalfaiteurs ne se privent pas d'utiliser pour déjouer les mécanismes de protection traditionnels. Dans ce contexte, de nombreux professionnels de l'IT peinent à suivre le rythme et à sécuriser leur infrastructure avec efficacité.

Évolution des cyberadversaires, ressources limitées, pénurie de talents, manque d'interaction entre des solutions de sécurité hétérogènes, distribution des applications et des données, problèmes de main-d'œuvre, coût et complexité des outils, exigences de conformité et de règlementation, manque de visibilité sur l'entreprise… les défis de cybersécurité sont multiples et concernent les structures de toutes tailles. Et tous ces facteurs empêchent les entreprises de planifier stratégiquement leur avenir.

Pour surmonter ces obstacles, elles peuvent se tourner vers des solutions clé en main efficaces et économiques telles les services de détection et réponse managées (Managed Detection and Response, MDR). En effet, une plateforme MDR assure une cybersécurité performante et économique nettement plus rapidement qu'en déployant un centre des opérations de sécurité (SOC) en interne.

AVANTAGES D'UNE SOLUTION MDR

L'adoption d'une solution adaptée apporte de nombreux avantages :

- Réduction des dommages et des temps d'arrêt, mise en œuvre d'approches de récupération structurées et amélioration des mesures de sécurité futures.
- Conservation de la pile de sécurité existante. Dans l'idéal, une solution MDR doit pouvoir s'intégrer à n'importe quel produit de sécurité. Cette intégration permet de protéger les investissements existants et d'adopter une stratégie des plus performantes. Elle garantit également une visibilité panoramique et une protection complète de votre écosystème numérique, ce qui permet de détecter proactivement les menaces et de réagir rapidement à un éventuel incident de sécurité.
- Réduction de la charge des équipes de sécurité. Un service MDR permet à votre équipe IT de se concentrer sur les projets métier essentiels au lieu de traquer des faux positifs. À la clé : un sentiment de satisfaction accru pour les employés.
- Réponse plus rapide aux menaces. Les produits MDR conjuguent des fonctions de chasse aux menaces automatique et humaine, des renseignements améliorés sur les menaces et une meilleure capacité de réponse aux incidents afin d'identifier les attaques plus rapidement tout en réduisant les délais de remédiation.
- Comblement du déficit de compétences en cybersécurité. En palliant le manque de compétences en cybersécurité, les services MDR contribuent à la continuité d'activité sans les problèmes de coût et de couverture inhérents au recrutement, à la formation et à la fidélisation de la main d'œuvre.
- Accès à une expertise spécialisée et à des outils avancés pour gérer des menaces sophistiquées et persistantes.
- Élargissement des zones de protection. Une solution MDR augmente la visibilité ainsi que la protection des terminaux distribués et des surfaces d'attaque tels que les appareils connectés (IoT) et les applications cloud.
- Accélération du retour sur investissement (ROI) et réduction significative des coûts de déploiement par rapport à la mise en œuvre d'un SOC en interne. Se reporter à la section « Création d'un SOC ou achat d'une solution MDR » pour de plus amples informations sur les coûts.

PRINCIPAUX FACTEURS À PRENDRE EN COMPTE

Les entreprises peuvent utiliser des services MDR pour améliorer les capacités de leur propre SOC ou se doter d'une solution clé en main pour toutes leurs opérations de cybersécurité. Mais tous les services MDR ne se valent pas. D'où l'importance de savoir quelles fonctionnalités rechercher pour faire le bon choix. De manière générale, un service MDR intègre les éléments suivants :

01 DÉPLOIEMENT EXTRÊMEMENT SIMPLE

La mise en œuvre d'un service MDR doit être simple et ne pas exiger le remplacement des outils de sécurité déjà en place. Il n'est pas nécessaire d'installer des capteurs au niveau des terminaux ni de modifier la pile de sécurité existante — sauf si vous le souhaitez. Avec un service MDR, les experts en cybersécurité se chargent du déploiement, de l'intégration et de la configuration à votre place.

02 PROTECTION AVANCÉE FONDÉE SUR L'IA

Un service MDR efficace s'appuie sur l'IA prédictive et l'apprentissage automatique (ML) pour surveiller et protéger tous les terminaux (ordinateurs, serveurs, appareils mobiles, systèmes locaux, hybrides et basés sur le cloud). Il utilise des renseignements propriétaires qui peuvent servir à analyser la télémétrie étendue en vue de détecter et de prévenir les menaces dès le début de leur cycle. Cette approche proactive permet de stopper les cyberattaquants tout en minimisant les alertes qui contribuent à la fatigue numérique des analystes. Les données, les opérations et la réputation de l'entreprise sont ainsi préservées.

03 GESTION CENTRALISÉE

Un service MDR fournit une vue d'ensemble de l'environnement de l'entreprise en unifiant les tâches de détection et de réponse d'un bout à l'autre de la pile de sécurité. Objectif : combler le manque de visibilité et couvrir les angles morts afin d'accélérer la réponse, le confinement et la remédiation des attaques sophistiquées.

04 INTÉGRATION À DES OUTILS TIERS

De nombreuses entreprises ne peuvent se permettre de remplacer leurs outils de sécurité. C'est pourquoi les solutions MDR doivent être compatibles avec les applications de sécurité les plus courantes. Les solutions MDR qui reposent sur une architecture ouverte de détection et réponse étendues (XDR) et des intégrations prédéfinies permettent d'adopter une stratégie de cybersécurité optimale.

05 ACCOMPAGNEMENT PAR DES PROFESSIONNELS DE LA CYBERSÉCURITÉ

Les services MDR permettent de bénéficier du concours de professionnels de la cybersécurité qui répondront à vos questions, formuleront des recommandations, personnaliseront les playbooks et aideront à tester les fonctionnalités de sécurité des nouveaux services et technologies. Il est recommandé de privilégier les prestataires de services MDR dont les collaborateurs affichent de nombreuses années d'expérience et qui, si possible, ont été récompensés dans le cadre de concours de cybersécurité.

TÉLÉMÉTRIE POUR PROTÉGER LES SURFACES D'ATTAQUE EN EXPANSION

06

Dans un contexte d'omniprésence du cloud, des communications mobiles et de l'Internet des objets, les solutions MDR doivent extraire les données de télémétrie d'un éventail élargi de surfaces d'attaque potentielles — terminaux, trafic réseau, applications cloud, SaaS, identités, courrier électronique — afin de distinguer les signes d'attaque des alertes inutiles avec plus de précision et de fournir des détections plus fidèles et des réponses plus rapides aux menaces.

RENSEIGNEMENTS SUR LES MENACES

07

Face à des auteurs de menaces qui modifient constamment leurs techniques, tactiques et procédures (TTP), les solutions MDR les plus efficaces s'enrichissent en permanence de nouveaux renseignements stratégiques, opérationnels et tactiques afin d'identifier les menaces et de neutraliser plus rapidement les attaques. Un service MDR doit également intégrer l'un des principaux référentiels de cybersécurité tels que MITRE ATT&CK®, SOC 2 ou le cadre de cybersécurité du NIST.

CHASSE AUX MENACES AUTOMATIQUE ET HISTORIQUE

08

Le service de sécurité MDR idéal intégrera une fonction de chasse aux menaces automatique et historique, ainsi qu'une capacité de détection adaptée aux exigences de votre entreprise. La détection automatisée des menaces permet de repérer et de confiner plus rapidement les fichiers et activités potentiellement malveillants avant qu'ils ne provoquent des dommages importants. Quant à la fonction de détection historique, elle fournit aux chasseurs des informations qui leur permettent d'identifier les menaces passées sur la base de nouveaux renseignements.

RÉPONSE AUX INCIDENTS

09

Un service MDR peut inclure une fonction complète de gestion et de réponse aux incidents (IR) qui couvre tous les types d'incidents, du vol de propriété intellectuelle aux ransomwares. La réponse aux incidents doit comporter des processus de planification, de récupération et de continuité, ainsi que des fonctions d'automatisation, d'identification et de confinement des compromissions, d'éradication des malwares, de récupération et de restauration de l'environnement du client. Elle doit également intégrer les enseignements tirés de ses expériences aux plans de réponse futurs.

ANALYSES FORENSIQUES NUMÉRIQUES

10

Un fournisseur de services MDR doit proposer des services d'analyse forensique numérique pour renforcer la capacité de réponse à incident. Ces services qui englobent l'identification, la collecte et l'analyse d'indices numériques pour non seulement recréer le « crime », mais également combler la faille de sécurité qui l'a rendu possible sont essentiels pour identifier les vulnérabilités et renforcer la posture de sécurité.

TRANSPARENCE TOTALE ET CONFORMITÉ

11

Le fournisseur de services MDR idéal doit être en mesure de démontrer sa conformité aux règlementations gouvernementales et sectorielles en matière de cybersécurité et de confidentialité, ainsi que sa maîtrise des exigences de conformité dans le secteur d'activité de ses clients.

ANTICIPATION DES COÛTS

12

Calculer le coût d'une solution MDR ne doit pas être compliqué. Pour éviter toute mauvaise surprise, les fournisseurs doivent proposer des prix comprenant la connexion à un nombre de capteurs illimité et l'utilisation de données illimitées pour permettre aux clients de gérer leurs dépenses avec une plus grande précision.

AVANTAGES POUR LES PARTIES PRENANTES

Une solution MDR apporte des avantages quantifiables à toutes les parties prenantes d'une entreprise.

SOC ET ÉQUIPE IT

- En réduisant le nombre de faux positifs, en agrégeant les données relatives aux menaces et en hiérarchisant les informations, un service MDR contribue **à réduire la fatigue numérique liée aux alertes** et permet aux équipes de se concentrer sur les menaces potentielles légitimes.
- Les services MDR ont été conçus pour **identifier les menaces et y répondre rapidement** grâce à une capacité de détection avancée fondée sur l'IA, aux renseignements sur les menaces, à une surveillance continue de l'environnement des clients et à une chasse aux menaces automatique et humaine.
- Pour assurer une détection **hautement précise des menaces**, les services MDR utilisent les données de télémétrie issues de toutes les surfaces d'attaque afin de distinguer les signes d'attaque des alertes inutiles avec plus de précision ainsi que de fournir des détections plus fidèles et des réponses plus rapides aux menaces.

RSSI

- Les services MDR **réduisent la charge de travail des équipes IT**, ce qui évite d'embaucher du personnel supplémentaire et permet aux professionnels de l'informatique en place de se concentrer sur leurs compétences et les objectifs stratégiques de l'entreprise.
- En s'intégrant aux solutions de cybersécurité déjà en place, une solution MDR **préserve la valeur des investissements** existants tout en renforçant la posture de sécurité globale.
- Une solution MDR assure **une visibilité et une protection complètes** de tout l'écosystème numérique en surveillant en permanence les réseaux, les terminaux, le cloud et les sources d'identité.
- Une solution MDR permet une détection proactive des menaces et **accélère la réponse aux incidents de sécurité potentiels**.

CEO/CFO/CIO

- Alors que le coût moyen d'une violation de données atteint 4,5 millions de dollars, une solution MDR axée sur la prévention **peut éviter aux entreprises** de perdre plusieurs millions de dollars en cas de cyberattaque.[2]
- Les services MDR assurent une couverture continue à un coût fixe, ce qui **permet aux entreprises d'économiser des sommes qu'elles** pourront consacrer à d'autres projets informatiques stratégiques.
- Les solutions MDR aident également les entreprises **à s'aligner sur les règlementations** en vigueur et à s'intégrer aux cadres de sécurité existants afin de respecter les exigences de conformité.

CRÉATION D'UN SOC OU ACHAT D'UNE SOLUTION MDR

Pour aider les entreprises à évaluer les avantages d'un service MDR, nous avons élaboré le modèle composite d'une société de taille moyenne. Objectif : comparer les sommes dépensées au cours de la première année pour créer un SOC de dimensions moyennes doté d'une équipe minimale au coût d'une solution MDR complète livrée clé en main. En fonction de la taille du SOC et du nombre de terminaux à protéger, une société peut économiser plusieurs millions de dollars en externalisant ses services de cybersécurité. En d'autres termes, une entreprise qui met en œuvre une solution MDR peut bénéficier d'une protection complète et d'une surveillance H24 moyennant un investissement 85 % moins élevé qu'en créant un SOC de toutes pièces.[3]

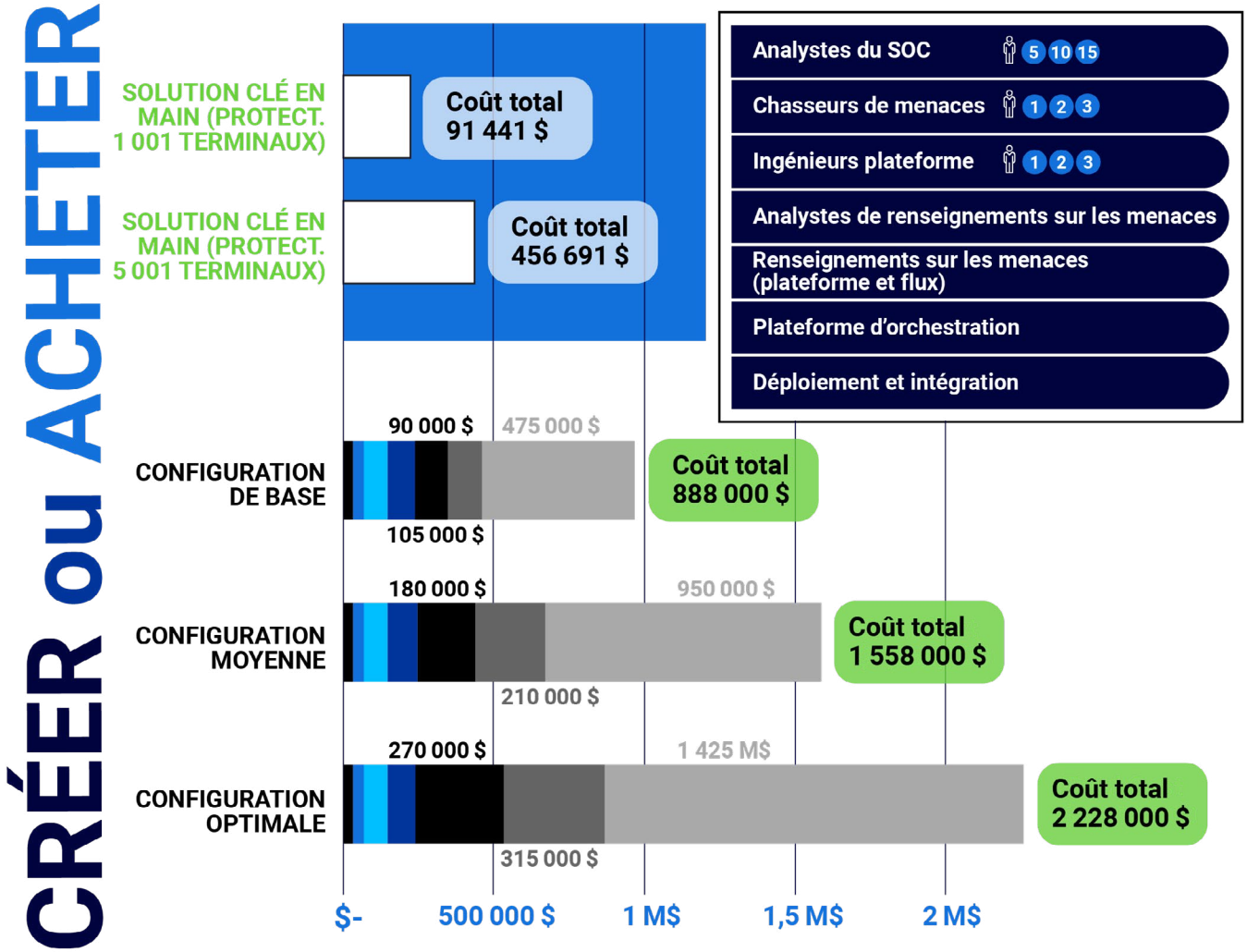

Figure 1 : Comparatif entre les coûts engendrés pour la création d'un SOC en interne et l'achat d'une solution MDR

CHECKLIST : CHOISIR UNE SOLUTION MDR ADAPTÉE

Capacités technologiques et de réponse, services, informations sur les fournisseurs, feuille de route… plusieurs éléments doivent être pris en compte lors de l'évaluation d'une solution MDR. Ceux-ci vous garantissent d'adopter une solution de cybersécurité capable de demeurer à la pointe du secteur en fonction de l'évolution des technologies et des menaces.

TECHNOLOGIES ET RÉPONSES

- Service de détection et neutralisation avancées des menaces fondé sur l'IA
- Architecture ouverte permettant d'utiliser des technologies provenant de différents fournisseurs
- Capacité à assimiler différentes sources de télémétrie, ce qui permet d'utiliser n'importe quel fournisseur et n'importe quelle technologie
- Mises à jour continues des technologies et renseignements contextuels sur les cybermenaces pour détecter et éliminer les nouvelles TTP
- Intégration de la cartographie MITRE ATT&CK®, de données tierces et de la télémétrie sur les menaces pour une meilleure protection
- Métriques opérationnelles plus rapides que la moyenne pour les délais moyens de détection (MTTD), d'identification (MTTI) et de remédiation (MTTR)
- Classification et hiérarchisation des alertes en fonction de règles et étiquettes, avec fonctionnalités automatisées pour réduire la fatigue numérique
- Sécurité complète sans consommation excessive de ressources de calcul (CPU)

SERVICES

- Couverture 24x7
- Équipe d'experts SOC possédant plusieurs années d'expérience et diverses certifications sectorielles
- Guides opérationnels (playbooks) de réponse adaptés à votre environnement
- Transparence totale sur le processus de sécurisation de votre entreprise
- Collaboration avec les équipes internes pour répondre aux questions, synchroniser les playbooks, proposer des exercices théoriques et techniques, et animer des formations pratiques
- Documentation relative aux exigences de conformité règlemetaires

FOURNISSEURS

- Historique général de l'entreprise et bilan
- Excellentes références clients
- Fournisseur établi avec un faible taux de rotation des employés et fort de nombreuses années d'expérience
- Engagement à atteindre, voire dépasser, les accords de niveau de protection (Protection-Level Agreement, PLA)
- Garantie contre les violations provoquées par un dysfonctionnement de la solution MDR

STRATÉGIE PÉRENNE

- Possibilité de maintenir ou de modifier avec flexibilité la pile de sécurité en place afin de maximiser les investissements existants
- Possibilité d'intégrer les produits de sécurité les plus performants
- Compréhension et prise en charge des nouvelles exigences règlementaires pour garantir la conformité
- Capacité à sécuriser un grand nombre et types de terminaux — y compris distants, mobiles et IoT —, et à gérer les règles d'utilisation des appareils personnels (BYOD)
- Authentification continue, accès conditionnel et autres technologies Zero Trust
- Feuille de route technologique sur trois ans pour illustrer les ajouts et mises à jour prévus par le prestataire de services MDR

CylanceMDR

UNE FLEXIBILITÉ ET UNE EXTENSIBILITÉ HORS PAIR

CylanceMDR™ est une solution de sécurité complète fondée sur l'IA de Cylance® et construite sur une architecture Open XDR avec des intégrations de capteurs immédiatement opérationnelles. Cette solution s'intègre aux solutions de sécurité et aux capteurs les plus courants, de sorte que les clients peuvent conserver les solutions qu'ils utilisent déjà. En outre, il n'est pas nécessaire de déployer de nouveaux agents ou logiciels — pas même les nôtres.

Nos experts primés complètent votre équipe pour combler le déficit de compétences en cybersécurité. Ils s'occupent des tâches de surveillance, de chasse aux menaces et de gestion des alertes entrantes pour permettre à vos collaborateurs de se concentrer sur les objectifs et les projets stratégiques de votre entreprise. Votre équipe bénéficie sans délai d'un soutien personnalisé de la part de nos experts-conseils.

CylanceMDR apporte des avantages qui ont fait leurs preuves dans différents secteurs d'activité :

- **Vaste écosystème d'intégrations prédéfinies.** CylanceMDR assure une surveillance, une détection et une réponse complètes, 24 heures sur 24 et 7 jours sur 7, d'un bout à l'autre de votre écosystème. Compatible avec les outils de sécurité dont vous disposez déjà, CylanceMDR collecte des données de télémétrie dans l'ensemble de vos surfaces d'attaque — terminaux, réseau, applications cloud, sources d'identités, logiciels SaaS et courrier électronique — afin de distinguer les signes d'attaque des alertes inutiles avec plus de précision, fournir des détections plus fidèles et des réponses plus rapides aux menaces, tout en palliant le manque de visibilité.
- **Sécurité exceptionnelle.** Fondée sur l'IA, CylanceMDR réduit les délais moyens de détection (MTTD), d'identification (MTTI) et de remédiation (MTTR) pour minimiser les faux positifs. Grâce aux solutions de cybersécurité BlackBerry®, CylanceMDR parvient à neutraliser plus de 98 % des menaces avant qu'elles ne compromettent votre environnement et ce, sans le moindre impact sur les performances. À noter également que les solutions de cybersécurité BlackBerry consomment près de 20 fois moins de ressources système que les produits concurrents.[4]
- **Expertise primée.** L'équipe CylanceMDR est composée de professionnels chevronnés et d'experts en chasse aux menaces qui affichent plus de 15 ans d'expérience dans le domaine de la cybersécurité. Leurs compétences ont été mises en lumière lors d'évènements tels que SOC X™ et DEF CON. Ces équipes font partie des rares structures mondiales à avoir participé aux deux évaluations MITRE pour la technologie MDR. En se consacrant à la sécurité de votre entreprise, les experts CylanceMDR permettent à votre équipe IT de se concentrer sur les fonctions métier essentielles.
- **Grande capacité de réponse et de restauration.** CylanceMDR dispose d'un service de réponse aux incidents complet qui fonctionne au-delà de la simple isolation des terminaux en incorporant des modèles de réponse automatisés, guidés et actifs. L'équipe chargée des analyses forensiques numériques et des réponses aux incidents (DFIR) supervise toutes les facettes de cette activité, du confinement et de l'éradication des menaces à la restauration des systèmes et à l'analyse des preuves numériques.

- **Rentabilité rapide.** CylanceMDR fournit un SOC de pointe dont le coût est 85 % inférieur à celui d'un centre des opérations de sécurité créé et géré en interne.[5] Sa mise en œuvre ne nécessite en général que quelques semaines au lieu de plusieurs mois, ce qui permet aux entreprises d'accélérer leur rentabilisation. En outre, selon Forrester, la solution BlackBerry offre un retour sur investissement de 293 % en six mois et permet de réaliser des économies de plusieurs millions de dollars sur trois ans.[6]

- **Économies.** L'architecture ouverte et agnostique de CylanceMDR protège les investissements que votre entreprise a déjà consacrés aux solutions de cybersécurité d'autres fournisseurs, avec à la clé une flexibilité et une évolutivité à l'épreuve du temps. Selon l'étude 2023 Total Economic Impact™ de BlackBerry consacrée à CylanceMDR[6] et publiée par le cabinet Forrester Consulting, les entreprises qui ont adopté cette solution ont réduit de 90 % les opérations de sécurité internes et de 90 % le temps nécessaire pour protéger de nouveaux actifs tout en utilisant moins de ressources humaines. De plus, les clients éligibles bénéficient d'une totale sérénité grâce à une garantie d'un million de dollars pour couvrir les dépenses résultant d'un incident de sécurité. Cette couverture étendue englobe les analyses forensiques, le paiement de cyberextorsions et les dépenses liées à un cyberincident.

- **Tarification prévisible.** Une tarification simplifiée qui englobe la connexion à un nombre illimité de capteurs et l'utilisation illimitée de données garantit le montant de vos dépenses sans mauvaise surprise. Les utilisateurs de CylanceMDR peuvent ainsi modéliser le coût total de possession des investissements consacrés à leur cybersécurité de manière simple et rapide.

- **Fin de la fatigue numérique.** Les analystes CylanceMDR s'appuient sur les solutions déjà en place et sur l'IA de Cylance pour réduire considérablement le nombre d'alertes envoyées aux clients. Notre équipe d'intégration optimise les agents installés sur les terminaux afin de réduire de 99,5 % le volume des alertes de sécurité[7], épargnant ainsi à vos collaborateurs la fatigue numérique liée aux alertes.

- **Conformité aux exigences règlementaires.** CylanceMDR répond aux exigences de conformité en s'alignant sur les règlementations en vigueur et en s'intégrant aux cadres de sécurité existants, comme le démontrent les évaluations de MITRE. En outre, ses capacités de détection fondée sur l'IA et de surveillance continue assurent une supervision complète et une documentation approfondie des incidents. Les experts SOC de CylanceMDR et les solides capacités de réponse à incident garantissent une action rapide et des rapports détaillés pour maintenir la conformité.

Pour en savoir plus sur CylanceMDR, demandez une démo.

Sources :

[1] https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

[2] https://www.ibm.com/reports/data-breach

[3] D'après les calculs effectués sur la base du coût total de création et de recrutement de personnel d'un SOC par rapport à l'achat de CylanceMDR (données de clients réels et conclusions d'analystes).

[4] https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/resources/blackberry-com/resource-library/en/cyber/2023/standard/rp/rp-tolly-group-cylanceendpoint-by-blackberry-comparative-endpoint-protection-test-report.pdf

[5] D'après les calculs effectués sur la base du coût total de création et de recrutement de personnel d'un SOC par rapport à l'achat de CylanceMDR (données de clients réels et conclusions d'analystes).

[6] Rebaptisée CylanceMDR, la solution CylanceGUARD® a été évaluée par le cabinet Forrester Consulting avant son changement de nom. Les résultats de l'évaluation s'appuient sur une entreprise composite. https://www.blackberry.com/content/dam/resources/blackberry-com/resource-library/en/cyber/2023/standard/rp/forrester-tei-of-cylanceguard.pdf

[7] Sur la base de calculs effectués en interne

BlackBerry. Intelligent Security. Everywhere.

BlackBerry (NYSE : BB ; TSX : BB) fournit des logiciels et des services de sécurité intelligents aux entreprises et aux gouvernements du monde entier. La société assure la sécurité de plus de 235 millions de véhicules actuellement en circulation. Basée à Waterloo (Canada), la société s'appuie sur l'intelligence artificielle et l'apprentissage automatique pour proposer des solutions innovantes dans les domaines de la cybersécurité, de la protection et de la confidentialité des données. BlackBerry est également leader dans les domaines de la sécurité et de la gestion des terminaux, du chiffrement, et des systèmes embarqués. La vision de BlackBerry est claire : assurer un futur connecté auquel vous pouvez faire confiance.

Pour toute information complémentaire, rendez-vous sur BlackBerry.com et suivez @BlackBerry.

BB24 | 240815