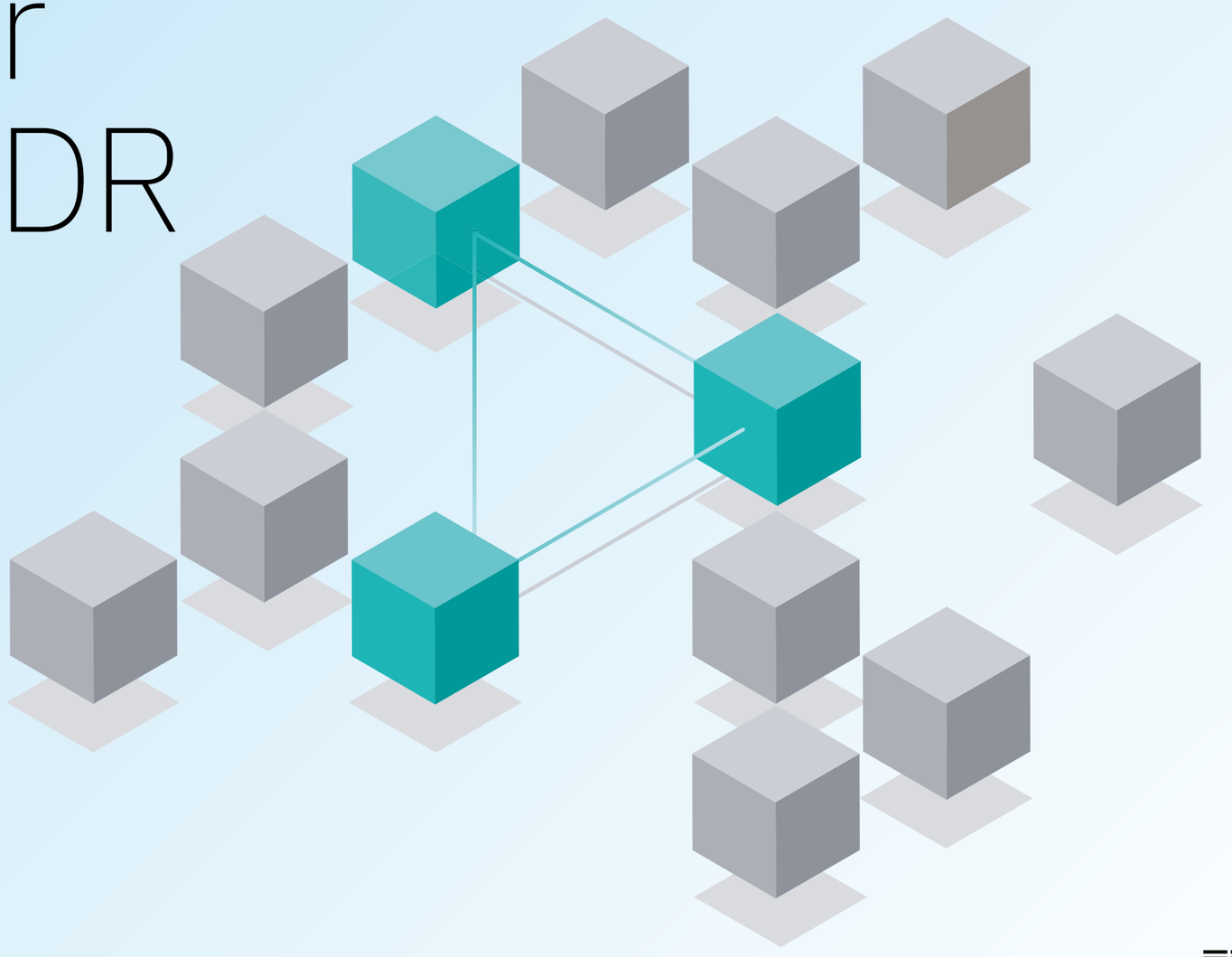
Guide de l'acheteur pour les solutions EDR

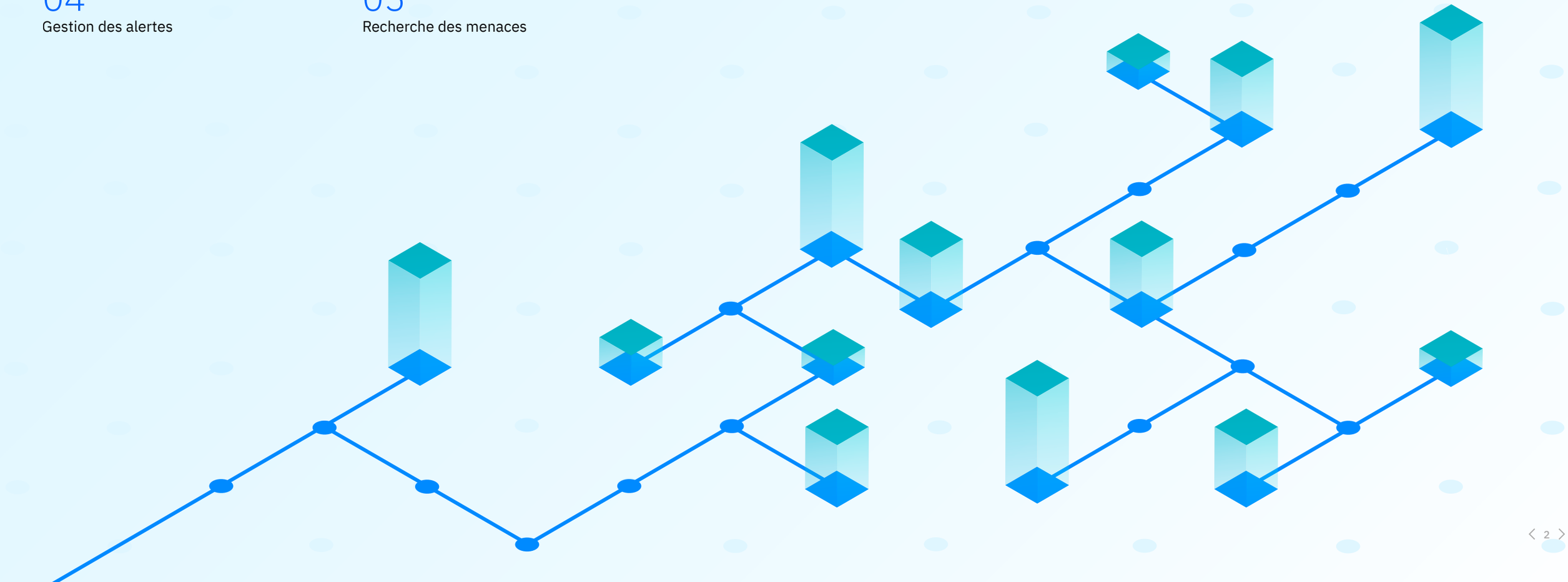
Comment choisir la meilleure solution de détection et réponse aux points de terminaison pour votre entreprise



REAQTA
an IBM Company

IBM

Sommaire



01
Introduction

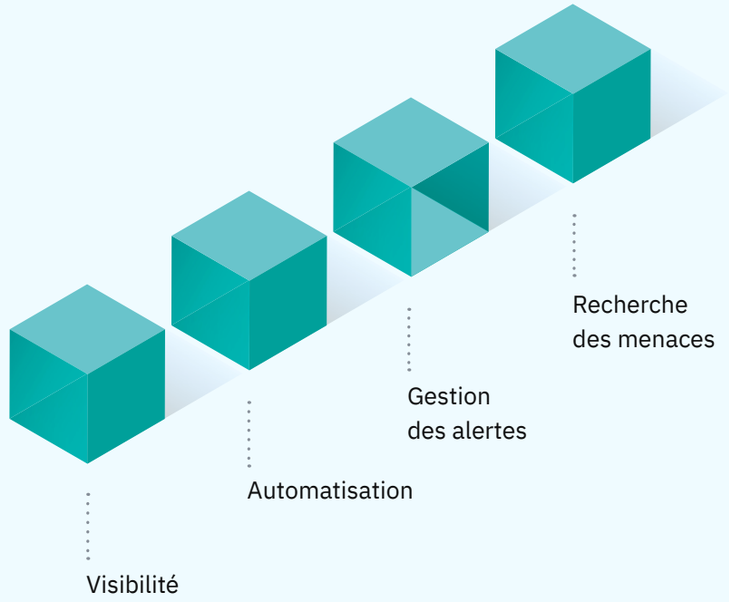
Qu’est-ce que l’EDR et pourquoi en ai-je besoin ?
Nous observons une augmentation de la prolifération et de l’interconnexion des points de terminaison et des données ces dernières années, associée à une hausse des activités d’acteurs malveillants. Ces facteurs créent une menace sérieuse pour l’activité des organisations qu’elles soient grandes ou petites. De plus en plus d’entreprises sont victimes d’attaques de cybercriminels et de groupes étatiques.

Les méthodes de protection conventionnelles combattent les menaces connues, mais sont perméables face aux techniques d’attaque sophistiquées et inconnues et n’offrent pas de visibilité sur les actifs, ce qui constitue l’un des principaux obstacles à la sécurisation de ces systèmes. Les compétences expertes en matière de protection aux points de terminaison ne sont généralement accessibles qu’aux organisations les plus grandes ou les mieux financées. Sachant que de nombreuses attaques se produisent désormais à la vitesse d’une machine et qu’elles se déplacent, les équipes humaines, qui s’appuient sur des solutions de protection conventionnelles des points de terminaison, ne peuvent plus faire face.

Une solution de détection et réponse aux points de terminaison (EDR) bloque et isole de façon préventive et automatique les logiciels malveillants tout en fournissant aux équipes de sécurité les bons outils pour relever ces défis avec confiance. Une solution EDR moderne permet la continuité de l’entreprise en atténuant efficacement les menaces automatisées et évoluées de plus en plus nombreuses, telles que les rançongiciels ou les attaques sans fichier, sans augmenter la charge de travail des analystes ou nécessiter des spécialistes de sécurité hautement qualifiés.

Êtes-vous confronté à ces défis ?
- Défaillance des solutions existantes
- Visibilité limitée
- Manque de personnel qualifié
- Fatigue d’alerte
- Menaces dormantes

Une solution EDR moderne et efficace comprend quatre éléments principaux que nous verrons dans les chapitres suivants :



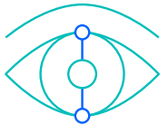
02
Visibilité complète sur vos points de terminaison

L'un des principaux obstacles à la sécurisation des points de terminaison est l'absence de visibilité. En tant que telle, une solution EDR moderne doit fournir une visibilité complète et approfondie des applications et des processus en cours d'exécution.

Lorsqu'une menace survient, une alerte en temps réel de son comportement, accompagnée d'un scénario graphique, doit être automatiquement créée alors que l'attaque se déroule, ce qui inclut une projection MITRE ATT&CK pour donner aux analystes une visibilité et une compréhension complètes sur l'événement.

La plupart, si ce n'est toutes les solutions logicielles de sécurité des points de terminaison, fonctionnent à l'intérieur du système d'exploitation, ce qui crée une limite pour l'agent du point de terminaison. Cela limite les capacités et la visibilité de l'agent tout en consommant plus de ressources informatiques. Avoir un agent qui travaille au niveau de la couche hyperviseur et qui est conçu pour être indétectable, non seulement minimise l'utilisation des ressources, mais fournit aussi une visibilité exceptionnelle pour surveiller tous les comportements des processus tout en restant invisible aux attaquants.

Que rechercher :
- Visibilité complète des points de terminaison
- Alertes en temps réel
- Création d'un scénario
- Agent sans friction
- Flux de travail unifié



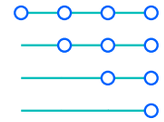
Question à poser :

→ Votre solution fournit-elle une visibilité complète et approfondie des applications et des processus en cours d'exécution ?

→ Lors d'une attaque, comment votre solution fournit-elle des informations utiles en temps réel pour mieux comprendre la menace ?

→ Outre la détection d'une brèche et le fait de vous alerter, votre MSSP fournit-il une réponse et une remédiation complètes ?

03
Automatisation et facilité d’utilisation



Sachant que les menaces sophistiquées et les périmètres de vulnérabilité vont aller croissant lors des prochaines années, de nombreuses organisations ont du mal à garder une longueur d’avance sur les cybercriminels. Une solution EDR moderne doit soulager une charge de travail élevée par une automatisation intelligente et facile à utiliser pour limiter le besoin de spécialistes sécurité hautement qualifiés.

La clé pour que les acheteurs tirent rapidement parti d’une solution EDR est d’automatiser et de simplifier. Grâce à l’automatisation de l’IA, la majeure partie du travail est laissée à des algorithmes qui minimisent les interactions humaines.

Avec de tels algorithmes d’IA, le logiciel devient plus facile à utiliser et les équipes peuvent être plus rapidement opérationnelles, sans une longue formation. Lorsqu’une attaque se produit, les temps de réponse sont critiques : le temps de l’enquête doit rester bien inférieur à la minute pour éliminer les menaces sophistiquées avant qu’elles ne puissent nuire à votre infrastructure.

Les acheteurs doivent rechercher une solution EDR susceptible de fonctionner en autonomie et d’offrir des capacités de détection et de réponse automatisées. Cette solution donne aux analystes une présentation claire en temps réel de l’attaque alors qu’elle évolue et peut offrir une remédiation guidée pour un retour rapide à la normale.

Que rechercher :
- Détection automatisée
- Remédiation guidée
- Analyses d’agent
- Temps de réponse rapides
- Facilité d’utilisation

Question à poser :

→ Des compétences avancées sont-elles requises pour exploiter la solution EDR ?

→ Pour réduire la charge de travail des analystes, la solution EDR est-elle capable de fonctionner en autonomie ?

→ En matière de temps de réponse, les menaces sont-elles analysées dans le cloud ou au niveau de l’agent ?

→ Si les menaces sont analysées dans le cloud, que se passe-t-il s’il n’y a pas de connexion Internet ?

04 Gestion des alertes

La principale différence entre une solution EDR et un antivirus (AV) conventionnel réside dans le fait que l'AV s'appuie sur des signatures disponibles pour la détection et qu'il doit connaître une menace pour pouvoir la bloquer. En revanche, une solution EDR utilise une approche comportementale pour identifier un logiciel malveillant et autres menaces potentielles selon la façon dont ils agissent sur un point de terminaison. Par ailleurs, contrairement à un AV, une solution EDR est légère par nature et ne nécessite pas de mises à jour fréquentes.

L'IA utilisée dans une solution EDR moderne doit donc être capable d'une détection rapide avec une grande précision et une haute fiabilité pour maintenir le volume des alertes (et la charge de travail des analystes) à un niveau minime. Les acheteurs doivent s'informer sur l'IA et les techniques d'apprentissage automatique utilisées. Comparée aux moteurs d'IA qui s'appuient sur des modèles préformés et une analyse pour la détection, une solution EDR qui utilise un modèle d'apprentissage initial pour définir le comportement normal de chaque point de terminaison offre une plus grande précision dans les détections et les alertes en cas d'écarts par rapport à la normale.

Pour réduire le temps de réponse et soulager la fatigue d'alerte des analystes, une solution EDR moderne doit être équipée d'un système de gestion des alertes robuste et basé sur l'IA, capable d'apprendre de l'analyste, puis d'appliquer en toute autonomie un processus décisionnel digne d'un analyste dans la gestion quotidienne des alertes. Le déploiement d'un système de gestion des alertes piloté par une IA entièrement automatisée est essentiel pour lutter contre la fatigue d'alerte, réduire les démissions de collaborateurs et reprendre le contrôle.

Que rechercher :
- Alertes de haute fiabilité
- Utilisation de modèles d'IA
- Prévention de la fatigue d'alerte
- Gestion automatisée des alertes

Question à poser :

→ Votre solution fournit-elle un moyen de gérer et de clore automatiquement les alertes ?

→ Comment votre solution libère-t-elle du temps pour les analystes ?

→ Comment votre solution réduit-elle les faux positifs ?

→ Si un collaborateur s'en va, comment ses connaissances de notre infrastructure seront-elles conservées ?

05
Recherche des menaces

La recherche des menaces est une partie importante d'une solution EDR moderne. Elle est indispensable au maintien d'un environnement propre dépourvu de menaces. La recherche de menaces peut rapidement établir si de nouvelles menaces pénètrent un environnement et identifier les points faibles. L'exploration des données vous permet de rechercher et d'éliminer les menaces dormantes, susceptibles de passer inaperçues, mais pouvant résider dans un environnement pendant des mois, voire des années, dans l'attente d'être utilisées par un attaquant.

Par nature, les menaces en mémoire et sans fichier sont difficiles à dépister et encore plus difficile à suivre lorsque les attaquants utilisent différentes variantes lorsqu'ils ciblent une grande infrastructure. Une solution EDR moderne doit automatiser le travail de recherche et utiliser l'exploration des données pour permettre aux équipes de sécurité de rechercher automatiquement des menaces partageant des similitudes comportementales et fonctionnelles avec d'autres incidents, en fournissant des résultats en quelques secondes.

La flexibilité dans la recherche des menaces est très importante. Les acheteurs doivent rechercher une solution EDR, qui non seulement offre une grande bibliothèque de détections préétablies pouvant être déployées immédiatement, mais aussi des routines personnalisées pouvant être facilement créées, sans nécessiter de connaissances en matière de script, pour des scénarios spécifiques propres aux besoins de sécurité d'une organisation.

La recherche de menaces est souvent comparée à la recherche d'une aiguille dans une botte de foin. Les recherches EDR doivent fournir des résultats complets et granulaires en temps réel en permettant d'accéder à des paramètres de recherche spécifiques et de les combiner de manière inclusive ou exclusive. Pour aider davantage les analystes et leur faire gagner du temps, les résultats doivent être affichés dans une interface utilisateur graphique (IUG) facile à comprendre, de sorte qu'ils puissent facilement et intuitivement rechercher un événement, depuis n'importe quel point de terminaison, à tout moment.

Que rechercher :
- Recherche des menaces dormantes
- Recherche automatisée
- Création de routines personnalisées
- Aucune compétence requise en programmation
- Exploration des données
- Capacités en temps réel
- Présentation graphique

Question à poser :

→ Les utilisateurs peuvent-ils créer leurs propres stratégies et routines de détection personnalisées ?

→ Pouvez-vous automatiser des scénarios de recherche de menaces ?

→ Offrez-vous une présentation graphique des recherches de menaces pour accélérer le tri ?

→ Des compétences en programmation sont-elles nécessaires pour créer des playbooks ?

Étapes suivantes

Pour en savoir plus sur IBM Security ReaQta et demander une démo.

Compagnie IBM France
17 avenue de l'Europe
92275 Bois-Colombes Cedex

Produit aux États-Unis d'Amérique
avril 2022