Guide du marché pour la détection et la réponse réseau

14 décembre 2022 - ID G00730869 - 34

Par **et 1 plus**Jeremy D'Hoinne, Nat Smith,

Le marché de la détection et de la réponse réseau se développe régulièrement et s'étend à de nouveaux cas d'utilisation, tels que l'IaaS. Les responsables de la sécurité et de la gestion des risques devraient donner la priorité à la notification d'échec de remise en tant que complément aux autres outils de détection, en se concentrant sur les faibles taux de faux positifs et la détection des anomalies que les autres contrôles ne couvrent pas.

Aperçu

Principales constatations

- Le marché de la détection et de la réponse réseau (NDR) continue de croître régulièrement à 22,5%, selon les dernières prévisions de sécurité de Gartner, malgré la concurrence accrue d'autres plates-formes.
- Au fur et à mesure que les premiers utilisateurs entrent dans une phase de renouvellement, les workflows de réponse aux incidents et d'orchestration gagnent en poids au cours de l'évaluation.

- Une poignée de fournisseurs de NDR captent la plupart de l'attention sur le marché. Les organisations ayant des cas d'utilisation spécialisés en matière de détection gagneraient à mélanger des fournisseurs connus avec des acteurs locaux émergents dans leurs listes restreintes.

Recommandations

Pour développer leurs capacités de détection et de réponse réseau , les responsables de la sécurité et de la gestion des risques devraient :

- Complétez les solutions de détection existantes en mettant en œuvre des outils de notification d'échec de remise pour détecter les comportements anormaux et fournir des capacités d'investigation pour les activités post-violation.
- Identifier les lacunes dans les pratiques actuelles de détection et d'intervention afin de déterminer si les anomalies que NDR peut détecter comblent les lacunes de détection les plus urgentes.
- Comparez les fournisseurs de rapports de non-remise en définissant des mesures rationalisées et en évaluant l'impact positif de ces outils de notification d'échec de remise sur la détection des menaces, la productivité des centres d'opérations de sécurité (SOC) et la réponse automatisée.

Hypothèses de planification stratégique

D'ici 2026, le pourcentage d'entreprises qui évaluent les capacités de notification d'échec de remise à partir de produits autonomes passera à 70 %, contre 90 % aujourd'hui.

D'ici 2027, plus de la moitié des détections de rapports de non-remise proviendront d'environnements cloud, contre moins de 10 % aujourd'hui.

D'ici 2027, la réponse automatisée à la détection des anomalies réseau ne dépassera pas 40% des anomalies détectées.

Définition du marché

Les produits de détection et de réponse réseau (NDR) détectent les comportements anormaux du système en appliquant une analyse comportementale aux données de trafic réseau. Ils analysent en permanence les paquets réseau bruts ou les métadonnées de trafic entre les réseaux internes (est-ouest) et les réseaux publics (nord-sud). La notification d'échec de remise peut être fournie sous la forme d'une

combinaison d'appliances matérielles et logicielles pour les capteurs, et d'une console de gestion et d'orchestration sous la forme d'un logiciel sur site ou SaaS.

Les organisations s'appuient sur la notification d'échec de remise pour détecter et contenir les activités post-violation telles que les ransomwares, les menaces internesou les mouvements latéraux. La notification d'échec de remise complète d'autres technologies, qui déclenchent des alertes principalement basées sur des règles et des signatures, en créant des modèles heuristiques du comportement normal du réseau et en détectant les anomalies.

Les principales fonctionnalités sont les suivantes :

- Possibilité de collecter l'activité du trafic brut
- Enrichissement des métadonnées au moment de la collecte ou lors de l'analyse des événements
- Facteurs de forme de déploiement compatibles avec les réseaux locaux et cloud
- Techniques d'apprentissage automatique (ML) pour établir une activité normale de base et détecter les comportements anormaux
- Agrégation des alertes en incidents de sécurité logiques en fonction de plusieurs facteurs, pas seulement de l'ID d'alerte et des alertes répétées
- Réponses automatisées, telles que le confinement de l'hôte (via l'intégration) ou le blocage du trafic

Description du marché

Des dizaines de fournisseurs prétendent analyser le trafic réseau (ou les enregistrements de flux) et détecter les activités suspectes sur le réseau.

Pour être compétitives dans les listes restreintes, les solutions NDR doivent :

- Analysez le trafic de paquets réseau brut ou les flux de trafic (par exemple, l'exportation d'informations de flux IP [IPFIX] ou les enregistrements NetFlow) en temps réel ou quasi réel.

- Surveillez et analysez le trafic nord/sud (lorsqu'il traverse le périmètre), ainsi que le trafic est/ouest (lorsqu'il se déplace latéralement sur le réseau).
- Être capable de modéliser le trafic réseau normal et de mettre en évidence le trafic suspect qui se situe en dehors de la plage normale pour les modèles de trafic nord/sud et est/ouest.
- Proposer des techniques comportementales (détection non basée sur les signatures), telles que le ML ou l'analyse avancée qui détecte les anomalies du réseau.
- Regroupez les alertes individuelles dans les incidents structurés pour faciliter les enquêtes sur les menaces.
- Fournir des capacités de réponse automatique ou manuelle pour réagir à la détection de trafic réseau suspect.

Les solutions NDR sont généralement exclues des listes restreintes lorsqu'elles :

- Nécessite un composant prérequis, par exemple, ceux qui nécessitent une plate-forme de gestion des informations et des événements de sécurité (SIEM) ou un pare-feu.
- Mettre l'accent sur la criminalistique réseau plutôt que sur la fonctionnalité de détection, principalement par le stockage et l'analyse des données PCAP (Full Packet Capture).
- Travailler principalement sur l'analyse des logs.
- Sont basés principalement sur l'analyse de l'activité de session utilisateur ou des événements d'annuaire d'utilisateurs qui sont principalementaxés sur l'analyse du trafic dans les environnements de l'Internet des objets (IoT) ou de technologie opérationnelle (OT), car des solutions spécialisées peuvent mieux répondre à ce cas d'utilisation.
- Manque de connaissance du marché de leurs capacités de NDR.

Selon la taille de l'organisation, la responsabilité NDR, une fois déployée, passe de l'infrastructure à l'équipe SOC, qui est chargée d'analyser les alertes et de gérer les réponses qui ne sont pas automatisées.

Direction du marché

Le marché NDR évoluera vers l'un ou l'autre de ces scénarios de plate-forme technique :

- **NDR** de réseau hybride : ils s'étendent plus profondément aux réseaux sur site existants ainsi qu'aux nouveaux environnements cloud, ajoutant de nouvelles techniques de détection qui les aident à éviter de devenir une fonctionnalité de l'infrastructure existante ou des produits de sécurité adjacents (tels que SIEM). La télémétrie de détection primaire proviendra toujours de l'analyse des modèles de trafic réseau, mais pourrait s'étendre au-delà en ajoutant d'autres types de détection, tels que les anomalies de posture de sécurité pour l'infrastructure cloud.
- **XDR :** La notification d'échec de remise pourrait contribuer à XDR en intégrant l'analyse des événements réseau . Les analystes de Gartner continuent de constater que la majorité des évaluations de non-remise concernent aujourd'hui des déploiements autonomes, mais cela pourrait changer rapidement à mesure que les plates-formes XDR progressent.
- **Banalisé dans le cadre** d'une autre plate-forme de sécurité: Le marché NDR peut devenir une caractéristique d'une plate-forme de sécurité consolidée. C'est ce qui est arrivé au sandboxing réseau il y a quelques années.

Rapport de non-remise sur réseau hybride

Les organisations qui ont investi dans NDR, en particulier les grandes, sont susceptibles de renouveler leurs contrats, car elles investissent dans la technologie. La majorité des demandes de notification d'échec de remise continuent d'inclure uniquement des cas d'utilisation de détection de réseau. La détection est forte et les flux de travail s'améliorent avec l'accent mis sur la feuille de route, ce qui permet de gagner du temps sur la réponse aux incidents et de mettre en évidence les causes profondes pour assurer une résolution correcte. Avec ce succès et cette confiance, les entreprises expérimentent de nouvelles fonctionnalités de notification d'échec de remise et étendent leur couverture pour inclure des zones du réseau qui ne sont pas initialement exposées à la notification d'échec de remise, en particulier pour voir tous les mouvements latéraux entre différents types d'infrastructure. La fragmentation des tableaux de bord est l'une des principales raisons qui pourraient empêcher NDR de poursuivre sa courbe de croissance, car les clients sont déjà aux prises avec le problème du « trop grand nombre de consoles ».

XDR

XDR en tant qu'architecture peut être décrit comme partageant certains aspects du SIEM, maisil porte une attente accrue de faire apparaître des événements nouveaux et précorrélés à partir de plusieurs types de capteurs. La technologie NDR peut contribuer à XDR en détectant les anomalies basées sur le réseau et en ajoutant et en corrélant ces événements dans le tableau de bord centralisé.

XDR sur le marché aujourd'hui est principalement un mouvement de consolidation (« plate-forme ») pour les fournisseurs avec plusieurs produits de sécurité. Les tendances à la consolidation des fournisseurs favorisent l'adoption de plates-formes plus grandes, avec moins de dépendance à l'égard des solutions ponctuelles. Les grands fournisseurs de sécurité réseau utilisent également de plus en plus le terme « XDR » lorsqu'ils communiquent la proposition de valeur de leurs consoles de gestion et de surveillance centralisées existantes. Les données de Gartner montrent que les demandes XDR sont souvent une demande pour comprendre le potentiel d'expansion des déploiements EDR (Endpoint Detection and Response) existants. Les offres consolidées, comme XDR, attirent souvent d'abord les entreprises de taille moyenne. Ces tendances sont les principaux moteurs pour que la technologie NDR devienne des composants d'une plate-forme/portefeuille XDR à l'avenir.

Les systèmes intégrés tels que XDR peuvent impliquer différentes parties prenantes, ce qui les rend plus complexes à déployer que les projets de notification d'échec de remise autonomes. Les enquêtes de Gartner sur la notification d'échec de remise mentionnent fréquemment la possibilité de déployer le rapport de non-remise en tant que solution de surveillance autonome sans dépendances; c'est un trait attrayant du marché du rapport de non-remise pour les grandes entreprises. Cependant, les frictions de déploiement et la concurrence entre les fournisseurs pour établir leur outil comme la solution « à panneau unique » pourraient empêcher l'architecture XDR de devenir l'évolution naturelle de NDR. Ces raisons s'ajoutent au défi plus traditionnel du « meilleur de sa catégorie » par rapport au « meilleur de sa catégorie ».

Technologie banalisée

Il existe un scénario dans lequel la notification d'échec de remise peut être absorbée par des dispositifs de sécurité multifonctions. La consolidation des fournisseurs est une option populaire pour les organisations avec des équipes plus petites, ou lorsque la valeur fournie ne justifie plus un produit dédié. Pour conserver un avantage en termes de détection d'anomalies sur le réseau, les fournisseurs doivent continuellement améliorer leur travail de science des données et de ML à mesure que les tactiques, les modèles de trafic et les habitudes de travail des attaquants évoluent. Les fournisseurs de NDR pure-play sont plus susceptibles d'investirune plus grande quantité de ressources pour améliorer les modèles ML connexes que les fournisseurs qui offrent NDR en tant que fonctionnalité, mais ils pourraient avoir du mal à rivaliser avec des plates-formes plus grandes, ce qui aura un impact sur leur capacité à se développer et donc à investir.

Pour que le marché de la notification d'échec de remise réussisse à long terme, les fournisseurs de NDR de réseau hybride doivent convaincre les organisations disposant d'une surface d'attaque réseau suffisante d'investir durablement et de conserver la notification d'échec de remise en tant que produit autonome. Pour ce faire, ils doivent démontrer que leurs analyses avancées peuvent détecter des anomalies plus pertinentes et disposent de capacités de réponse aux incidents plus fortes.

Analyse du marché

NDR a montré sa flexibilité dans la surveillance du trafic réseau partout où les utilisateurs et les charges de travail existent, car la popularité croissante des arrangements de travail à domicile a déplacé les modèles de trafic sur site d'est en ouest vers le nord-sud. En conséquence, de nombreux fournisseurs ont accéléré le développement de leurs produits pour aller au-delà du centre de données et du campus traditionnels sur site.

Lorsque le marché NDR était naissant, il était composé d'un mélange de startups pure-play et de sociétés de surveillance de réseau s'étendant aux cas d'utilisation de la sécurité. Au fur et à mesure que le marché se développe, il attire de grands fournisseurs de plates-formes et des fournisseurs de sécurité qui offrent des produits de détection des violations multifonctions.

L'un des avantages de la technologie NDR est la capacité de ses consoles de gestion et de surveillance à faciliter les flux de travail de réponse aux incidents. Les agrégations d'événements et les vues prédéfinies réduisent la courbe d'apprentissage et offrent une visibilité appréciée par les petites équipes de sécurité.

Certains fournisseurs privilégient une transparence totale dans leurs flux de travail, ce qui permet aux analystes experts en sécurité d'examiner les détails granulaires qui peuvent être utilisés pour une portée plus poussée et une inspection plus approfondie de la criminalistique. Les organisations qui disposent des ressources, des compétences et du temps nécessaires pour travailler intensivement avec la criminalistique apprécieront ces fournisseurs de rapports de non-remise qui se concentrent sur la chasse, les cadres d'attaque et l'utilisation et le stockage à long terme de la télémétrie de l'investigation réseau. La transparence et la flexibilité de ces solutions de notification d'échec de mise au marché se font généralement au détriment de la simplicité et de la facilité d'utilisation.

En revanche, d'autres fournisseurs de rapports de non-remise se concentrent fortement sur le cas d'utilisation de détection des menaces, en centrant leurs tableaux de bord de surveillance sur l'explicabilité d'un incident de sécurité et en rationalisant leur flux de travail de réponse aux incidents avec autant d'automatisation que possible. Les organisations disposant d'équipes de sécurité plus petites bénéficieront

immédiatement des capacités de détection améliorées et tireront probablement parti des réponses automatisées et d'autres mesures d'atténuation. Ces solutions faciles à utiliser et polies ont tendance à fournir un retour sur investissement rapide et nécessitent moins d'interaction humaine.

Tendances récentes du marché NDR

Gartner constate que de nombreuses offres de rapports de non-remise se sont étendues pour capturer de nouvelles catégories d'événements et analyser des modèles de trafic supplémentaires. Cela comprend :

- **Nouveaux capteurs** : en créant ou en intégrant des capteurs de point de terminaison, tels que l'EDR, en ingérant des journaux tiers tels que SIEM, en analysant les événements logiciels/plateformes/infrastructure-as-a-service via leurs API de surveillance, ou en ajoutant la prise en charge des cas d'utilisation OT.
- **Nouvelles techniques** de détection : en ajoutant la prise en charge des signatures plus traditionnelles, la surveillance des performances, les renseignements sur les menaces et parfois les moteurs de détection des logiciels malveillants. Cette évolution vers une détection réseau plus multifonction s'aligne bien avec le cas d'utilisation de la convergence des opérations réseau/sécurité, mais aussi avec les entreprises de taille moyenne.
- **Automatisation du flux de travail de réponse** aux incidents : les technologies de notification d'échec de remise regroupent déjà les événements anormaux individuels en incidents de sécurité. En enrichissant les alertes pour fournir un meilleur contexte et en appliquant le ML pour semi-automatiser le processus de réponse aux incidents, les fournisseurs de rapports de non-remise encouragent les grandes équipes SOC à s'appuyer davantage sur la console NDR, plutôt que de transférer les alertes directement à un SIEM.
- **Rapport de non-remise géré** : Certains des grands fournisseurs ont commencé à offrir plus de services en plus du produit NDR et des abonnements, allant des notifications proactives des fournisseurs en cas d'incident à la détection des menaces entièrement gérée. Bon nombre de ces services sont récents et pris en charge par des équipes petites mais en pleine croissance.
- **Architecture évolutive** : de plus en plus de fournisseurs fournissent désormais des analyses ML uniquement dans le cloud, car l'approche centralisée facilite l'amélioration des détections ML.

Quelques-uns des fournisseurs de NDR ont construit un portefeuille de sécurité au-delà du marché NDR et exploitent leurs connaissances en matière de détection d'anomalies dans de nouveaux domaines (par exemple, SaaS ou sécurité de messagerie). Ces fournisseurs repositionnent leur proposition de valeur avec le ML en son cœur, et le réseau devient l'un des cas d'utilisation de cette approche analytique.

Récemment, Gartner a observé des fournisseurs émergents tirant parti de nouvelles approches (par exemple, Cynamics, Nétography) ou se concentrant sur des cas d'utilisation cloud (CloudCover), se différenciant des autres fournisseurs de NDR, tout en leur faisant concurrence pour des cas d'utilisation similaires.

« Réponse » ne signifie pas toujours « remédiation »

En étudiant les listes de présélection de NDR, Gartner remarque que la majorité des candidats s'identifient comme NDR, ce qui laisse entendre que les limites du marché NDR se sont solidifiées au fil du temps. Les fournisseurs citent fréquemment les fournisseurs SIEM comme concurrents, et parfois les systèmes de détection d'intrusion (IDS) open source. En effet, le R dans NDR est plus proche de la réponse aux incidents que le R dans EDR ou XDR, ce qui est plus susceptible de définir des attentes en matière de « correction » automatisée.

En outre, de nombreux fournisseurs de rapports de non-remise identifient leurs produits comme de bons outils pour les équipes de recherche de menaces et incluent des capacités de recherche sophistiquées, ciblées sur les intervenants en cas d'incident. Ces caractéristiques de la composante « réponse » définissent la technologie NDR autant que ses capacités de détection.

Au cours des derniers mois, Gartner a remarqué une légère augmentation du nombre d'organisations intéressées par la réponse automatisée, mais ces organisations souhaitent souvent une portée étroite. Dans de nombreux cas, les cas d'utilisation acceptables pour la réponse automatisée basée sur le réseau sont les modèles de trafic nord-sud liés (communication C2, exfiltration de données) ou le mouvement latéral des rançongiciels. Des améliorations plus notables sont visibles grâce à l'intégration avec d'autres contrôles de sécurité, sur les tableaux de bord de surveillance et sur l'automatisation du flux de travail de réponse aux incidents.

L'approche intelligente de NDR en matière de « réponse » consiste à prendre en charge le flux de travail de réponse aux incidents grâce à l'agrégation d'événements, à l'automatisation du flux de travail et à la connaissance contextuelle. Si nécessaire, il bloque ou contient également les activités malveillantes. La capacité d'un fournisseur individuel à fournir un faible taux de faux positifs et des capacités d'enquête efficaces encourageront les clients à adopter les capacités de réponse du fournisseur.

Les fournisseurs et les produits NDR continuent de se multiplier

En plus des fournisseurs inclus dans l'étude (voir Note 1), les analystes de Gartner voient un nombre croissant d'autres fournisseurs avec une offre NDR (voir Note 2). Certains pays pourraient abriter de nombreux fournisseurs de NDR, tels que la Chine (Hillstone Networks, Huawei, QI-ANXIN, Sangfor, Tencent, Tophant, Venustech et autres) ou la France (Allentis, CUSTOCY, Gatewatcher , Nano Corp, SEKOIA. IO, Sesame IT, TEHTRIS et autres). Les grands fournisseurs de sécurité sont également plus susceptibles d'offrir des produits NDR dans le cadre de leur portefeuille.

Fournisseurs représentatifs

Les fournisseurs énumérés dans ce Guide du marché n'impliquent pas une liste exhaustive. Cette section vise à fournir une meilleure compréhension du marché et de ses offres.

Introduction sur le marché

Le tableau 1 comprend une liste de fournisseurs représentatifs (voir la note 2 pour les autres fournisseurs de rapports de non-remise suivis par Gartner).

Tableau 1 : fournisseurs représentatifs en matière de détection et de réponse réseau

Nom du fournisseur	***Produit Nom***
Réseaux Arista	Arista NDR
Cisco	Analyse de réseau sécurisée Analyse cloud sécurisée

Nom du fournisseur	***Produit Nom***
Éclairage de base	Plateforme de notification d’échec de remise ouverte Corelight
Darktrace	Darktrace DETECT Darktrace RÉPONDRE
ExtraHop	Révéler(x)
Fidelis Cybersécurité	Réseau Fidelis
Gardien	AionIQ
Gigamon	Gigamon ThreatINSIGHT
IronNet	Plateforme de défense collective IronNet
Plixer	Plateforme de renseignement de sécurité Plixer

Nom du fournisseur	***Produit Nom***
Progrès	Système de détection d’anomalies Flowmon
QI-ANXINE	SkyEye
Sangfor	Commandement cybernétique
Réseaux Stamus	Plate-forme de sécurité Stamus
Tencent	Rapport de non-remise T-Sec
Trellix	Détection et réponse du réseau Trellix
Tendance Micro	Trend Micro Deep Discovery Trend Micro TippingPoint Trend Micro Vision One
Vectra	Plateforme de détection et de réponse aux menaces Vectra

Nom du fournisseur	Produit Nom
VMware (en anglais)	Détection et réponse de NSX Network

Source : Gartner (décembre 2022)

Profils des fournisseurs

Réseaux Arista

Arista Networks est un fournisseur mondial de réseaux et d'infrastructures, qui vend principalement des rapports de non-remise aux États-Unis et dont le siège social est situé à Santa Clara, en Californie. Le produit NDR d'Arista Networks (Arista NDR) est basé sur l'acquisition d'Awake Security en 2020. Arista propose également des services gérés (Arista managed NDR service).

Arista collecte principalement des données à partir de capteurs, qui peuvent être autonomes ou intégrés dans des commutateurs Arista. Arista NDR inclut un moteur de recherche de chasse aux menaces, basé sur un langage propriétaire (Adversarial Modeling Language [AML]). Arista cible les réseaux à grande échelle et propose des intégrations avec les principaux fournisseurs et hyperviseurs IaaS pour mieux servir les équipes réseau et sécurité avec une visibilité accrue pour les cas d'utilisation des centres de données.

La tarification d'Arista NDR inclut les coûts matériels lors de l'utilisation d'appliances physiques et une gamme d'abonnements pour les capteurs virtuels et les déploiements IaaS, avec des niveaux de bande passante basés sur le trafic agrégé (nord-sud et est-ouest).

Cisco

Cisco est un fournisseur mondial basé à San Jose, en Californie. Le portefeuille de Cisco comprend deux produits en compétition dans les listes restreintes de rapports de non-remise : Secure Network Analytics (SNA), un outil principalement sur site, et Secure Cloud Analytics (SCA), un rapport de non-remise fourni dans le cloud.

Les produits Cisco NDR peuvent collecter NetFlow/IPFIX à partir de capteurs tiers ou du fournisseur. L'architecture SNA est une architecture à trois niveaux, avec Flow Collector agrégeant les flux de plusieurs capteurs avant d'envoyer des événements à la console de gestion centralisée avec un moteur d'analyse hébergé dans le cloud en option. Cisco SCA utilise des API natives pour collecter des événements IaaS et peut être déployé en tant qu'agent sur un pod Kubernetes. Les produits Cisco NDR privilégient l'heuristique, l'analyse statistique et les renseignements sur les menaces, combinés à des règles prédéfinies de violation de politique et de seuil pour détecter les anomalies de réseau et de sécurité.

Cisco s'intègre déjà à de nombreux composants d'infrastructure Cisco, tels que le moteur de services d'identité de Cisco, et continue d'étendre son intégration NDR avec SecureX, leur console de surveillance centralisée qui fait appel aux opérations réseau et de sécurité.

L'approche tarifaire de Cisco en matière de notification d'échec de remise peut être légèrement différente pour SCA et SNA, mais pour les deux, le coût dépend du nombre d'environnements surveillés et du volume d'événements collectés.

Éclairage de base

Corelight est un fournisseur mondial, basé à San Francisco, en Californie. Corelight est le résultat de l'effort de construire un produit commercial sur le dessus des moteurs Zeek et Suricata. Le produit NDR du fournisseur, Corelight Open NDR, fournit une capture sélective complète des paquets (Smart PCAP) et a récemment publié une console d'analyse et de gestion SaaS (Investigator).

Corelight NDR (Open NDR) s'appuie sur son propre matériel et ses capteurs virtuels (y compris VM sur les plates-formes IaaS) pour collecter des données. Il propose une VM de gestion de capteurs (Fleet Manager). Les détections de rapports de non-remise ouvertes sont principalement basées sur des règles, exploitant leurs propres règles et moteurs de détection pour l'heuristique, et utilisant des ensembles de règles complémentaires de partenaires tels que CrowdStrike et Proofpoint. L'analyse ML, principalement réalisée par Corelight Investigator dans le cloud, est disponible en mettant l'accent sur les modèles de trafic nord-sud. Le fournisseur continue de cibler les grandes organisations, visant non seulement à effectuer des analyses en temps quasi réel, mais également à améliorer leurs capacités d'investigation pour les réseaux à grande échelle.

Les prix Corelight combinent les coûts matériels traditionnels pour les appliances physiques avec les coûts d'abonnement pour des moteurs supplémentaires ou des flux de renseignements sur les menaces, en fonction de la bande passante requise.

Darktrace

Darktrace est un fournisseur mondial de rapports de non-remise dont le siège social est situé à Cambridge, au Royaume-Uni. Le rapport de non-remise de Darktrace, maintenant connu sous le nom de Darktrace DETECT, s'appelait auparavant Enterprise Immune System (EIS). Il reste leur produit phare, avec un abonnement séparé pour la réponse automatisée (Darktrace RESPOND, anciennement Antigena). Le fournisseur a récemment lancé Darktrace PREVENT, qui comprend la gestion de la surface d'attaque externe et l'analyse des chemins d'attaque.

Darktrace NDR collecte principalement des données à partir de son propre matériel, de capteurs virtuels et de capteurs de terminaux, mais peut également collecter des données à partir de produits de sécurité des terminaux et de l'infrastructure. Darktrace DETECT peut tirer parti d'API tierces pour enrichir ses propres analyses. Le fournisseur inclut plusieurs moteurs de détection, avec un fort accent sur l'apprentissage non supervisé pour la détection des anomalies. Darktrace s'est également diversifiée en surveillant le cloud (IaaS), les applications (SaaS), le courrier électronique et les réseaux OT et en appliquant ses techniques ML pour automatiser le processus d'enquête sur les incidents (appelé Cyber AI Analyst).

La tarification de la notification d'échec de remise de Darktrace est basée sur le nombre d'adresses IP surveillées, avec des coûts d'abonnement pour les modules de détection et de réponse, mais aussi pour des options supplémentaires, telles qu'un service de notification. Le fournisseur a récemment commencé à inclure les coûts matériels lors de l'utilisation de capteurs.

ExtraHop

ExtraHop est un fournisseur mondial de réseau et de sécurité avec des racines dans la surveillance des performances réseau, avec une majorité de ses ventes de NDR provenant des États-Unis aujourd'hui. Le siège social d'ExtraHop est situé à Seattle, dans l'État de Washington. ExtraHop Reveal(x) est la plate-forme de notification d'échec de remise du fournisseur , disponible en mode SaaS ou reposant sur des appliances physiques ou virtuelles pour l'analyse et la gestion. Le fournisseur propose désormais principalement son architecture d'analyse SaaS, appelée Reveal(x) 360.

ExtraHop Reveal(x) collecte des données à partir de ses capteurs appliances, d'infrastructures tierces et d'API de visibilité des paquets de plate-forme IaaS. Reveal(x) combine plusieurs techniques de détection, y compris les signatures et l'heuristique. Le fournisseur a récemment ajouté des articles interactifs sur les renseignements sur les menaces (Threat Briefing). Reveal(x) et Reveal(x) 360 fournissent des analyses statistiques et d'apprentissage automatique supplémentaires, effectuées dans le cloud et basées sur des événements anonymisés agrégés. ExtraHop fournit en option des capacités de déchiffrement du trafic et de capture complète des paquets (ce qui nécessite des périphériques de stockage de paquets supplémentaires pour les organisations souhaitant conserver les données locales), qui peuvent ensuite être consultées directement à partir du moteur de recherche de métadonnées (« vue Enregistrements »). Pour une réponse automatisée, ExtraHop s'intègre à divers fournisseurs, notamment Endpoint, SIEM et SOAR.

ExtraHop Reveal(x) comprend plusieurs niveaux d'abonnement, dont certains incluent des analyses en temps réel, des capteurs physiques, le stockage de métadonnées ou un stockage PCAP complet dans le cloud.

Fidelis Cybersécurité

Fidelis Cybersecurity est un fournisseur mondial, qui vend principalement des rapports de non-remise aux États-Unis, dont le siège social est situé à Bethesda, dans le Maryland. Le produit NDR du fournisseur s'appelle Fidelis Network et obtient la plupart de ses ventes auprès de clients basés aux États-Unis, suivis par EMEA. Fidelis Cybersecurity est disponible en tant que plate-forme de gestion et de capteurs entièrement sur site, mais une option SaaS pour la gestion est également disponible.

Fidelis Network peut ingérer des données provenant de capteurs dédiés et de diverses sources tierces, y compris des enregistrements de flux, des événements EDR et des journaux Active Directory, pour aider à détecter les menaces. Le système peut analyser via une gestion sur site ou basée sur le cloud. Fidelis Network comprend un moteur de recherche de métadonnées de chasse aux menaces. Le trafic crypté peut être analysé via JA3 ou déchiffré dans un processus de l'homme du milieu. Suricata est intégré dans le produit avec ses signatures pour la détection. Les moteurs d'analyse de Fidelis Network sont fortement axés sur l'analyse de contenu, l'apprentissage automatique étant utilisé pour améliorer la détection des logiciels malveillants, le sandboxing et la prévention des fuites de données. D'autres méthodes d'analyse sont disponibles, telles que l'heuristique et les renseignements sur les menaces.

La tarification de Fidelis Cybersecurity est basée sur une combinaison de bande passante agrégée surveillée sur tous les capteurs et du nombre de jours de conservation des métadonnées.

Gardien

Gatewatcher est un fournisseur régional de NDR, basé à Paris, en France. La notification d'échec de remise de Gatewatcher, appelée AionIQ, peut être déployée sur un serveur ou en tant que machine virtuelle. Il combine des capteurs matériels pour les cas d'utilisation sur site et des capteurs virtualisés avec la prise en charge de l'IaaS d'Amazon Web Services. Le portefeuille du fournisseur comprend également un IDS appelé Trackwatch, destiné à la surveillance des infrastructures critiques locales. Gatewatcher a commencé à se développer à l'international.

Le moteur d'analyse AionIQ comprend un moteur d'analyse de fichiers qui repose sur un antivirus tiers, un bac à sable, des signatures IDS, des renseignements sur les menaces et un ML supervisé pour détecter les activités malveillantes. AionIQ permet une réponse automatisée en tirant parti des intégrations d'API.

En plus des coûts matériels pour le capteur, et éventuellement pour le serveur de gestion, le logiciel AionIQ nécessite un abonnement avec une structure de prix décroissante basée sur le nombre d'actifs découverts.

Gigamon

Gigamon est un fournisseur mondial, vendant principalement NDR aux États-Unis, dont le siège social est situé à Santa Clara, en Californie. Le produit NDR de Gigamon, ThreatINSIGHT est principalement vendu aux États-Unis et en Australie. Gigamon inclut un service appelé DiN Guided-SaaS, qui fournit une approche dirigée de la notification d'échec de remise et tire parti de l'expérience du personnel de Gigamon en matière de réponse aux incidents.

Gigamon collecte principalement des données à partir de capteurs dédiés, physiques et virtuels. Ila également des intégrations avec certains fournisseurs EDR et peut ingérer des journaux tiers. Toutes les analyses sont effectuées dans le cloud. La chasse aux menaces fait partie de l'offre, en mettant l'accent sur la chasse guidée. Le trafic crypté est analysé via des signatures JA3, des techniques propriétaires et un décryptage de l'homme du milieu. Le fournisseur privilégie l'heuristique pour la détection des menaces suivie d'un ML supervisé. Gigamon utilise par défaut une période de rétention de 365 jours pour toutes les métadonnées. Suricata a été intégré pour aider à la détection des attaques basée sur les signatures.

La tarification Gigamon est basée sur le débit réseau analysé, ainsi que sur le coût des capteurs. Il n'y a pas de coût supplémentaire pour le service Guided-SaaS.

IronNet

IronNet est un fournisseur mondial de NDR coté à la Bourse de New York (IRNT) et dont le siège social est situé à McLean, en Virginie. La solution NDR d'IronNet est fournie via la plate-forme de défense collective d'IronNet. Il comprend deux composants principaux, IronDefense, qui inclut toutes les capacités de détection et d'analyse, et IronDome, qui est une communauté collaborative de clients IronNet NDR. IronDome facilite le partage sécurisé de la détection et de l'analyse avec les pairs afin d'améliorer la compréhension d'une équipe SOC dans le paysage actuel des menaces.

Laplate-forme de défense collective ronNet utilise à la fois des paquets réseau et des enregistrements de flux réseau, ainsi que des journaux provenant de services d'annuaire, de DNS et d'une large gamme d'autres produits de sécurité (par exemple, pare-feu, NAC, SIEM, EPP et autres). IronNet peut également fonctionner avec des journaux provenant de plates-formes IaaS. IronNet Collective Defense Platform utilise le ML ainsi qu'une analyse statistique importante pour la détection, mais une grande contribution à ses détections provient des communautés de défense collective, où les clients peuvent échanger des renseignements sur les attaques en temps quasi réel, identifiant les attaques avancées ou uniques au fur et à mesure qu'elles se déroulent, telles que les infrastructures C2 nouvelles ou auparavant inconnues.

IronNet évolue d'une tarification basée sur le débit à un schéma plus moderne par utilisateur à trois niveaux. Le premier niveau, Log Analytics, fournit une détection de base à partir de l'analyse des journaux. Le deuxième niveau ajoute la détection réseau et IronDome pour la collaboration communautaire. Ce niveau est le plus comparable aux autres produits NDR. Le niveau Entreprise est le plus cher et ajoute des capacités de chasse et des services améliorés supplémentaires.

Plixer

Plixer est un fournisseur mondial de NDR, dont le siège social est situé à Kennebunk, dans le Maine. Plixer est en train de redéfinir son portefeuille de produits. Le fournisseur a commencé comme un fournisseur de performances réseau, avec un produit appelé Plixer Network Intelligence (PNI, anciennement connu sous le nom de Plixer Scrutinizer). Plixer NDR est appelé Plixer Security Intelligence (PSI) Platform. Les deux produits peuvent utiliser les mêmes capteurs pour la collecte de données.

Plixer NDR surveille principalement le trafic via les enregistrements de flux réseau (NetFlow ou IPFIX) collectés sur site auprès des collecteurs de données, mais peut également ingérer des sources IaaS. Une partie de l'analyse s'exécute directement sur le collecteur de données et l'analyse basée sur le ML est effectuée sur une appliance dédiée (matérielle ou virtuelle) qui peut être déployée sur site ou dans le cloud. Plixer peut ingérer n'importe quel flux de renseignements sur les menaces à l'aide de STIX/TAXII et apporte également du contexte provenant de sources multiples, y compris les terminaux, les serveurs DNS, les pare-feu et les journaux des systèmes de prévention des intrusions (IPS).

La tarification Plixer est basée sur le nombre de sources qui exportent les enregistrements de flux réseau, telles que les routeurs, les commutateurs, les pare-feu et les VPC cloud. Pour maximiser l'économie, Gartner recommande d'utiliser des sources d'exportation consolidées à débit plus élevé au lieu de plusieurs sources à débit plus petit.

Progrès (Flowmon Networks)

Progress, un fournisseur mondial de développement d'applications et d'expérience numérique, est coté au Nasdaq (PRGS) et son siège social est situé à Burlington, dans le Massachusetts. Le fournisseur a acquis Flowmon Networks, un fournisseur mondial de rapports de non-réponse, grâce à l'acquisition de sa société mère Kemp Technologies en 2021. La solution NDR de Progress est le système de détection des anomalies Flowmon (ADS). La solution Flowmon ADS se compose de deux composants principaux. Le premier est un collecteur requis qui stocke, traite, analyse et visualise les données réseau. La seconde est une sonde facultative utilisée pour exporter des données de flux réseau et des métadonnées étendues. Cette architecture est également utilisée pour la gamme de produits de surveillance et de diagnostic des performances réseau Flowmon de Progress.

Flowmon ADS utilise principalement les enregistrements de flux réseau pour la détection et l'analyse, mais peut également utiliser les journaux des services d'annuaire. Flowmon Collector est le référentiel pour les enregistrements de données de flux et prend en charge plusieurs formats de flux, y compris IPFIX. Les enregistrements de flux peuvent être générés en mode natif à partir de périphériques d'infrastructure réseau conformes, ou les sondes de Flowmon peuvent être utilisées sur un port SPAN ou un TAP réseau pour générer des enregistrements IPFIX enrichis , y compris des informations IDS écrites sur l'extension IPFIX de Flowmon. Flowmon utilise une variété de méthodes, y compris l'analyse statistique, l'heuristique et le ML, les flux de renseignements sur les menaces et les signatures IDS.

La tarification de la solution NDR de Progress est basée sur différentes mesures de trafic, telles que le nombre d'enregistrements de flux traités, la bande passante ou la capacité de stockage.

QI-ANXINE

QI-ANXIN est un fournisseur régional, basé à Pékin, en Chine. QI-ANXIN propose une suite de produits de sécurité, y compris SkyEye, son produit de détection des menaces, qui est en concurrence sur le marché des rapports de non-remise. QI-ANXIN concentre actuellement ses efforts sur son marché domestique et a commencé à se développer à l'international.

SkyEye s'appuie fortement sur un large ensemble de règles, qui comprend une combinaison de signatures traditionnelles et de détection plus générique, basée sur l'apprentissage automatique supervisé. SkyEye comprend des capteurs d'appareils physiques et un bac à sable (qui fait partie de sa gamme de produits TSS). Le déchiffrement TLS (Transport Layer Security) est disponible pour le trafic vers les serveurs internes. Le fournisseur exploite également plusieurs sources de renseignements sur les menaces.

Le modèle de tarification de SkyEye inclut les coûts matériels pour les capteurs de l'appliance physique, la mise à niveau logicielle et les abonnements, y compris un abonnement à la mise à jour des renseignements sur les menaces.

Sangfor

Sangfor est un fournisseur mondial d'informatique et de sécurité, axé sur la notification d'échec de remise régionale, basé à Shenzhen, en Chine. Sangfor Cyber Command est la plate-forme analytique centralisée du fournisseur, collectant les événements des capteurs et autres produits Sangfor.

Sangfor Cyber Command combine plusieurs techniques de détection, y compris le ML supervisé et non supervisé, les signatures plus traditionnelles et les renseignements sur les menaces. Sangfor Cyber Command ne fournit pas de décryptage TLS natif, mais peut repérer les anomalies en analysant les métadonnées TLS. La réponse est disponible via l'intégration avec le pare-feu ou la passerelle Web sécurisée du fournisseur, mais aussi avec des pare-feu tiers et des produits de sécurité des terminaux.

Cyber Command est fréquemment associé à d'autres produits de sécurité du portefeuille de Sangfor. Le modèle de tarification des capteurs suit le modèle d'achat de matériel traditionnel. Des abonnements sont disponibles, notamment pour les mises à jour de la « base de données de sécurité ». Sangfor fournit également des services gérés qui s'appuient sur le produit Cyber Command.

Réseaux Stamus

Stamus Networks est un fournisseur mondial de rapports de non-remise dont le siège social est situé à Indianapolis, dans l'Indiana et à Paris, en France. La solution de notification d'échec de remise de Stamus est Stamus Security Platform et est disponible en deux niveaux : Stamus Network Detection and Response (NDR) et Stamus Network Detection (ND). Stamus ND comprend la détection de base de Suricata, le triage et la chasse aux menaces. Stamus NDR ajoute des renseignements personnalisables sur les menaces, une hiérarchisation automatisée des alertes et des analyses basées sur le ML.

Stamus Networks est fortement investi dans l'évolution de Suricata et, en tant que tel, utilise des paquets réseau complets comme source de données principale. Les capteurs Stamus (logiciels et matériels) peuvent prendre en charge les déploiements sur site et IaaS et alimenter le serveur central Stamus (logiciel). L'analyse commence avec le moteur Suricata dans les capteurs Stamus. Stamus peut déployer ses propres capteurs Suricata ou, dans de nombreux cas, peut utiliser vos capteurs Suricata existants . L'analyse comprend également le ML, l'analyse statistique, les renseignements sur les menaces et l'heuristique.

La tarification Stamus est basée sur le débit. Les licences annuelles pour Stamus Security Platform sont basées sur le nombre de capteurs et le débit global. Les capteurs sont disponibles avec des vitesses de liaison de 100 Mbps à 40 Gbps.

Tencent

Tencent est une grande société mondiale de technologie Internet, basée à Shenzhen, en Chine. Tencent propose un portefeuille complet de produits et services de sécurité (T-Sec), avec une gamme de produits NDR petite mais en croissance (T-Sec NDR), principalement proposée aux grandes entreprises en Chine. T-Sec NDR est principalement déployé en tant qu'appliances physiques, mais prend également en charge les environnements IaaS avec VM et les options de déploiement logiciel.

T-Sec NDR collecte des paquets complets et inclut la possibilité de stocker des PCAP pour l'analyse médico-légale, en plus de la détection en temps quasi réel. Il peut déchiffrer le trafic TLS et combine plusieurs moteurs de détection, y compris un bac à sable malveillant. Certaines détections ML sont disponibles et le fournisseur continue d'étendre son utilisation, mais T-Sec NDR combine principalement des renseignements sur les menaces, des signatures et des politiques basées sur des seuils pour détecter les anomalies. Son module de réponse s'appelle Tianmu. T-SEC NDR tire également parti de l'intégration avec Tencent et les produits de sécurité tiers.

La tarification de Tencent pour le rapport de non-remise T-Sec prend en charge un modèle de sécurité réseau traditionnel avec des ventes d'appliances à l'avance, mais évolue vers un modèle d'abonnement à plusieurs niveaux avec des fonctionnalités telles que le sandboxing, la capture de paquets complets et des capacités d'investigation supplémentaires disponibles dans les niveaux supérieurs.

Trellix

Trellix est un fournisseur mondial de sécurité d'infrastructure dont le siège social est situé à Plano, au Texas, issu de la fusion en 2022 des fournisseurs de sécurité établis McAfee Enterprise et FireEye.

La solution de notification d'échec de remise Trellix se compose de la console de gestion et de surveillance (Trellix Network Investigator) qui peut être déployée en tant que produit autonome avec ses propres capteurs, ou en plus des déploiements existants des produits de l'entreprise : Trellix NX (anciennement FireEye), Trellix IPS (anciennement McAfee NSP) et Trellix Network Forensics. Trellix NDR utilise principalement des paquets réseau pour la détection, mais peut également exploiter les enregistrements de flux réseau, ainsi que les journaux du DNS. Trellix utilise à la fois l'apprentissage automatique supervisé et non supervisé pour compléter l'analyse statistique, l'heuristique, les signatures IDS et les renseignements sur les menaces. Trellix NDR utilise l'analyse de session multiflux héritée de son moteur FireEye MVX via des environnements de système d'exploitation émulés pour recomposer le trafic réseau et obtenir la perspective de l'hôte cible. La technologie de sandboxing Trellix est également disponible pour fournir une analyse des logiciels malveillants.

Trellix NDR inclut une tarification basée sur l'utilisateur et le débit. Des frais distincts sont nécessaires pour les appliances, le matériel et les appliances virtuelles.

Tendance Micro

Trend Micro est un fournisseur mondial dont le siège social est situé à Tokyo, au Japon. Le produit NDR de Trend Micro est basé sur sa plate-forme Vision One, qui utilise Deep Discovery et TippingPoint comme capteurs réseau. L'APAC et la région EMEA sont des marchés clés pour Trend Micro.

Trend Micro collecte principalement des données à partir de capteurs matériels et logiciels, mais peut également ingérer les journaux des pare-feu et les alertes de son produit EDR. Le produit NDR de Trend Micro inclut la chasse aux menaces par le biais de son moteur de recherche, basé sur un langage propriétaire et une approche clé en main pour trouver les menaces. Le fournisseur privilégie les renseignements sur les menaces

et les signatures IPS pour la détection des menaces. Un grand nombre de signatures est disponible car le système utilise le moteur TippingPoint pour IPS. Trend Micro cible l'intégration avec son portefeuille de produits de sécurité existant, et les clients utilisant Vision One obtiennent une corrélation entre plusieurs produits.

La tarification de Trend Micro est basée sur l'achat de capteurs, dont les coûts varient en fonction du débit. Une licence d'entrée de télémétrie pour l'ingestion de rapports de non-remise est disponible moyennant des frais supplémentaires.

Vectra

Vectra est un fournisseur mondial de NDR, dont le siège social est situé à San Jose, en Californie. Le NDR de Vectra, maintenant connu sous le nom de Vectra Threat Detection and Response Platform, (anciennement appelé Vectra Cognito) est leur produit phare. Le fournisseur propose également une offre complémentaire de détection et de réponse gérées (MDR), appelée Vectra MDR. Vectra a récemment enrichi son portefeuille avec un produit d'évaluation de la posture de sécurité pour M365, suite à l'acquisition de Siriux Security Technologies au début de 2022.

Vectra Threat Detection and Response Platform analyse principalement les paquets réseau avec des capteurs d'appliances matérielles et des capteurs logiciels virtuels. Vectra travaille également directement avec certaines API SaaS et les journaux des services d'annuaire IaaS cloud pour fournir une détection et une réponse aux menaces pour ces cas d'utilisation. Vectra NDR s'appuie sur plusieurs moteurs de détection mettant fortement l'accent sur le ML et les méthodes d'apprentissage profond pour les détections basées sur le comportement. Un flux propriétaire de renseignements sur les menaces est intégré à l'analyse, et les clients peuvent également importer leurs propres flux de menaces.

La tarification de Vectra inclut la prise en charge des paquets, des API et des journaux, ainsi que tous les algorithmes de détection, les capacités de réponse et les interfaces utilisateur. La tarification est principalement basée sur le nombre d'adresses IP surveillées et comprend un nombre illimité de capteurs virtuels et cloud. Des schémas de tarification distincts sont utilisés pour les fonctionnalités facultatives, telles que les gigaoctets par jour pour le stockage médico-légal.

VMware (en anglais)

VMware est un fournisseur mondial qui vend principalement des rapports de non-remise aux clients de son hyperviseur ESX lorsqu'ils utilisent également NSX comme commutateur virtuel. Le siège social de VMware est situé à Palo Alto, en Californie. Le produit NDR de VMware, NSX

Network Detection and Response, est une acquisition de Lastline.

VMware collecte les données de la carte d'interface réseau virtuelle (vNIC) dans l'hyperviseur, si elle est concédée sous licence pour NSX, ainsi qu'à partir de la passerelle NSX pour irewall et des capteurs NSX. Pour les clients fortement investis dans l'exécution de leurs charges de travail sur les hyperviseurs VMware, il s'agit d'un moyen efficace d'ingérer des données réseau, car NSX ne nécessite pas de capteurs matériels. Le trafic ingéré peut être analysé sur site ou dans le cloud. Le trafic chiffré est analysé de plusieurs façons, y compris l'analyse propriétaire, les signatures JA3 et le déchiffrement TLS.

Pour détecter les menaces, NSX NDR utilise une combinaison de techniques, notamment le ML supervisé et non supervisé, les signatures IPS et un moteur de détection des logiciels malveillants. Le moteur IPS de NSX NDR est basé sur Suricata et inclut un grand nombre de signatures.

La tarification VMware de NSX NDR offre plusieurs options. Il peut être acheté en tant que module complémentaire à son produit NSX-T, basé sur des processeurs. Il peut être inclus dans le cadre d'un contrat de licence d'entreprise qui regroupe la sécurité réseau, la sécurité des terminaux et d'autres produits de sécurité. Il est également disponible en tant que produit autonome basé sur des processeurs.

Broadcom a annoncé son intention d'acquérir VMware en mai 2022. À la date de publication, VMware continuait de fonctionner en tant qu'entité indépendante. Gartner fournira des informations et des recherches supplémentaires aux clients à mesure que de plus amples détails seront disponibles concernant l'acquisition.

Recommandations du marché

Les entreprisesdoivent fortement envisager des solutions de notification d'échec de remise pour compléter les outils basés sur les signatures et les bacs à sable réseau. De nombreux clients de Gartner ont signalé que les outils de notification d'échec de remise ont détecté un trafic réseau suspect que d'autres outils de sécurité de périmètre avaient manqué.

Lors de l'évaluation des fournisseurs de rapports de non-remise, évaluez les facteurs suivants :

- Pure-play versus NDR en tant que fonctionnalité — Est-il plus judicieux d'implémenter NDR en tant que fonctionnalité d'un autre fournisseur de technologie (par exemple, SIEM ou XDR), ou avez-vous besoin d'une solution de NDR plus complète et pure-play de l'un des fournisseurs analysés dans ce guide du marché?

- **Détection —** Les détections de rapports de non-remise reposent sur une combinaison de techniques. Certains produits NDR sont solides car ils combinent plusieurs techniques; d'autres reposent principalement sur une seule technique (ML, renseignement sur les menaces ou signature). Concentrez-vous sur les types de détection et considérez une mesure telle que le « pourcentage d'incidents critiques détectés par NDR » pour comparer les solutions de NDR.
- **Réponse :** certains fournisseurs se concentrent davantage sur les réponses automatisées (par exemple, l'envoi d'une commande à un pare-feu pour supprimer le trafic suspect), tandis que d'autres se concentrent davantage sur les réponses manuelles (par exemple, en fournissant des outils puissants de chasse aux menaces).
- **Intégration —** Lorsque le produit NDR détecte un problème, l'alerte doit-elle être envoyée à sa console ou peut-elle être envoyée à un outil tiers pour l'alerter ? Existe-t-il une intégration avec des produits d'application tiers, tels qu'un pare-feu d'entreprise ou un produit de contrôle d'accès réseau ?
- **IT versus** OT **—** Le fournisseur peut-il s'intégrer aux cas d'utilisation OT ?

En outre, les responsables de la sécurité chargés d'évaluer et de comparer les fournisseurs de rapports de non-remise doivent d'abord définir des métriques rationalisées. Ces mesures sont plus pertinentes pour les systèmes de détection tels que la notification d'échec de remise qui devraient déclencher un nombre d'alertes plus faible. Les dirigeants doivent également évaluer comment la notification d'échec de remise modifie la définition de « suffisamment bon » pour la détection des menaces, la productivité SOC et la réponse automatisée. Des exemples de tels paramètres incluent « pourcentage d'incidents critiques détectés par NDR » ou « réduction moyenne du temps moyen d'enquête sur les incidents/faux positifs ».

Note de bas de page 1
Sélection du fournisseur représentatif

Ces fournisseurs ont été sélectionnés parce qu'il y avait suffisamment de preuves recueillies qu'ils répondaient à la définition et aux exigences de Gartner mises en évidence dans la section « Description du marché ».

Note de bas de page 2
Autres fournisseurs suivis par les analystes de Gartner

Cette liste de fournisseurs n’est pas exhaustive. En plus de la liste ci-dessous, lesfournisseurs de sécurité l arge sont également susceptibles d’offrir des produits NDR dans le cadre de leur portefeuille.

- Adhérent
- Allentis
- aizoOn (Aramis)
- Blue Hexagon (acquis par Qualys en octobre 2022)
- BluVector
- CloudCover
- Réseaux cPacket
- Cryptoimage
- GARDE
- CyGlass
- Cynamics
- Instinct profond
- Exeon
- Fortinet
- GREYCORTEX
- Réseaux Hillstone

- Huawei (en anglais)
- Prises de vues réelles
- LogRhythm
- Lumu Technologies
- Mode Mixage
- Muninn
- NANO Corp
- Netographie
- NetWitness
- SuivantRayon
- Nominet
- OpenText (Bricata)
- Ordr
- Quad Miners
- Qihoo 360
- Sésame IT
- Cyber stellaire
- TEHTRIS

- ThreatBook
- ThreatWarrior
- Tophant
- Vehere
- Venustech
- Verizon

peuvent pas être utilisées comme contribution à la formation ou au développement de l’intelligence artificielle générative, de l’apprentissage automatique, des algorithmes, des logiciels ou des technologies connexes.

Gartner