Progress® Flowmon®

# Une cybersécurité résiliente grâce à la détection et à la réponse du réseau

LIVRE BLANC

# Résumé

L'une des principales responsabilités des équipes de direction des entreprises consiste à identifier les facteurs de risque dans l'ensemble de leurs activités et de leurs opérations, puis à atténuer ces risques afin d'éviter les chocs ou les incidents qui pourraient avoir un impact sur les opérations à l'avenir. En 2023, la menace des cyberattaques constitue l'un des risques les plus importants auxquels sont confrontées les entreprises.

Les menaces de cybersécurité auxquelles sont confrontées les entreprises de tous types et de toutes tailles sont nombreuses, complexes et en constante évolution, les cybercriminels concevant et découvrant sans cesse de nouvelles méthodes d'attaque. Les équipes dirigeantes doivent s'assurer que leurs équipes de cybersécurité internes ou, plus fréquemment dans le contexte actuel, leur fournisseur de services de sécurité managés (MSSP) prend toutes les mesures de cyberdéfense nécessaires pour protéger 24 heures sur 24 et 7 jours sur 7 le personnel, les clients, les données et les systèmes informatiques.

La protection des personnes et des systèmes informatiques d'une entreprise contre les cyberattaques nécessite une approche à plusieurs niveaux qui déploie des solutions technologiques et des connaissances d'experts à de multiples endroits. Des protections doivent être mises en place au niveau des périmètres des réseaux, des terminaux des utilisateurs, des serveurs d'application et des services basés sur le Cloud, qui constituent une méthode de déploiement de plus en plus courante.

L'expérience de ces dernières années, au cours desquelles des protections ont été déployées et utilisées dans tous les lieux énumérés ci-dessus, a permis d'identifier un autre élément essentiel d'un dispositif de défense complet en matière de cybersécurité. Il s'agit de la nécessité de surveiller 24 heures sur 24 et 7 jours sur 7 l'activité sur le réseau d'une entreprise afin d'identifier toute activité qui s'écarte de la normale, puis de réagir rapidement pour empêcher les cyberattaques de s'installer sur les systèmes informatiques et de se propager.

Les solutions de détection et de réponse du réseau (NDR) ont émergé pour combler les lacunes en matière de protection de la cybersécurité mises en évidence par l'expérience. Les analystes du secteur, tels que Gartner et Quadrant Knowledge Solutions, considèrent que la NDR est essentielle à la défense de la cybersécurité, non pas comme une panacée pour toutes les menaces de cybersécurité, mais comme un élément central de la défense multicouche mentionnée ci-dessus.

Dans la suite de ce livre blanc, nous aborderons les défis auxquels les équipes de cybersécurité sont confrontées, nous expliquerons comment la NDR les aide à se défendre contre les attaques, nous résumerons le point de vue de Gartner et de Quadrant Knowledge Solutions sur le marché et les solutions NDR, nous décrirons l'évaluation par Gartner et Quadrant Knowledge Solutions de la solution NDR de Flowmon, nous donnerons des exemples concrets grâce aux études de cas des clients de Flowmon et nous expliquerons comment vous pouvez rapidement essayer (gratuitement !) le système de détection d'anomalies de Flowmon (Flowmon ADS) sur votre réseau (Flowmon ADS est notre produit NDR).



© 2024 Progress. Tous droits réservés.

Le principal enseignement pour les dirigeants ? Demandez à votre équipe de défense de cybersécurité si elle utilise la NDR et comment elle s'intègre dans votre stratégie plus large de défense de cybersécurité.

# Les défis auxquels sont confrontées les équipes de cybersécurité

Les menaces auxquelles les équipes de cybersécurité doivent faire face et qu'elles doivent prévenir ne semblent pas près de s'atténuer. Les attaques par ransomware et l'exfiltration de données sont en effet les types d'attaques auxquels la plupart des entreprises sont confrontées, les menaces persistantes avancées (APT) étant également utilisées par les cybercriminels d'État à des fins d'espionnage industriel. Le rapport Sophos State of Ransomware 2022 (voir le lien dans la section « Références ») montre que sur 5 600 entreprises interrogées dans 31 pays, deux tiers ont été touchées par des ransomwares au cours de l'année écoulée. Parmi les entreprises attaquées, 65 % ont dû traiter des données que les attaquants avaient cryptées - 43 % de celles qui ont détecté une attaque par ransomware ont donc dû nettoyer les retombées par la suite. Le coût moyen du rétablissement après une attaque était de 1,4 million de dollars, le paiement moyen aux cybercriminels s'élevant à 812 360 dollars, et le temps nécessaire pour se remettre de l'attaque était en moyenne d'un mois.

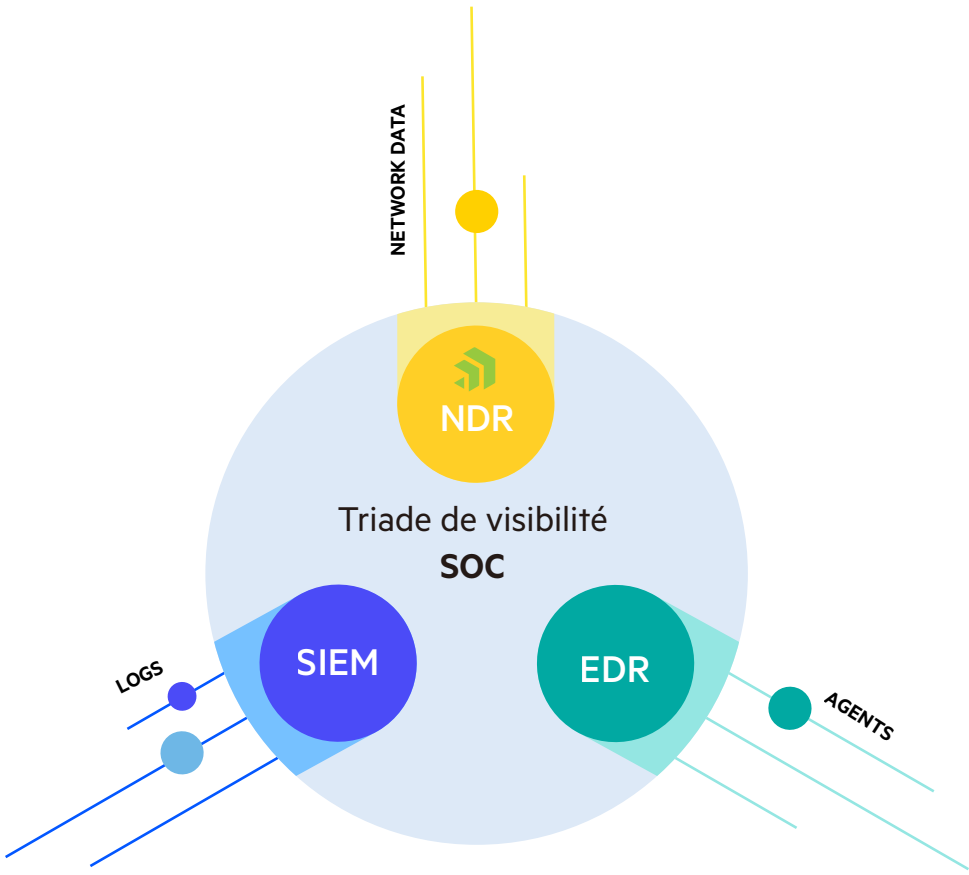
Les ransomwares ne constituent pas l'unique menace à laquelle il faut faire face, bien sûr. Le rapport de Sophos souligne également que les entreprises interrogées ont constaté une augmentation de 57 % du volume de tous les types de cyberattaques, mais que les ransomwares et le vol de données sont les menaces les plus importantes à l'heure actuelle. Le paysage des menaces s'est considérablement élargi depuis 2020. De plus en plus de personnes travaillent aujourd'hui à distance, et il semble que ce changement va se répercuter de manière permanente sur la façon dont les gens travaillent. Le travail hybride est la nouvelle norme. Pour les systèmes informatiques en réseau et leur défense, cela signifie que le trafic provenant de sources externes (souvent appelé trafic nord-sud) est plus important que celui provenant de sources internes/du réseau de l'entreprise (appelé trafic est-ouest).

Les professionnels de la cybersécurité ont déployé de nombreux outils technologiques pour se défendre contre les attaquants. Il s'agit notamment de protections périmétriques et périphériques telles que les pare-feux, la protection des dispositifs par EDR (Endpoint Detection and Response) ou SIEM (Security Information and Event Management) et les solutions SOAR (Security Orchestration, Automation and Response) pour automatiser la collecte des événements de sécurité et des logs provenant de l'ensemble des systèmes informatiques d'une entreprise afin de repérer les anomalies qui pourraient être des indicateurs de compromission d'une cyberattaque et d'y répondre.


© 2024 Progress. Tous droits réservés.

Ces outils défensifs existants sont toujours nécessaires dans le cadre d'une stratégie de défense globale. Mais le paysage des menaces est en constante évolution et les attaquants cherchent toujours de nouveaux moyens de contourner les protections de cybersécurité existantes, et de nouveaux exploits de type « zero-day » sont fréquemment découverts et corrigés par les fournisseurs de logiciels et de matériel. Chaque fois qu'une nouvelle faille est publiée, les attaquants tentent de l'exploiter avant que les équipes informatiques n'aient eu le temps de mettre à jour leurs systèmes pour la corriger. De plus, les données montrant le nombre élevé d'attaques réussies qui contournent les mesures de sécurité existantes et persistent ensuite sur les systèmes informatiques pendant une longue période avant d'être détectées montrent qu'il est nécessaire de renforcer les moyens de défense en matière de cybersécurité.

Les analystes de Gartner ont créé la triade de visibilité SOC pour illustrer comment la NDR constitue désormais un élément essentiel d'une stratégie de défense en matière de cybersécurité et comment elle s'articule avec le SIEM et l'EDR, qui sont plus connus. SOC est l'acronyme de Security Operations Centre (centre d'opérations de sécurité). Les SOC sont essentiels à la protection 24 heures sur 24 et 7 jours sur 7 qu'exigent les réseaux modernes, car ils se concentrent sur la surveillance des réseaux et des systèmes et sur la réaction à toute attaque ou activité suspecte. Les SOC peuvent être dotés d'un personnel 24 heures sur 24 et 7 jours sur 7, selon des schémas de travail par roulement, et permettent une protection 24 heures sur 24 afin de contrecarrer les cyberattaquants qui travaillent à l'échelle mondiale et pas seulement pendant les heures de bureau dans un fuseau horaire particulier.





© 2024 Progress. Tous droits réservés.

Comme le montre le diagramme ci-dessus, la NDR est axée sur l'analyse des données du réseau. En revanche, le SIEM analyse les données des logs (et d'autres informations système), et l'EDR surveille et protège les terminaux à l'aide d'agents et d'autres technologies. Les solutions de NDR ont émergé des solutions existantes de surveillance réseau pour ajouter une autre couche cruciale aux défenses en fournissant aux équipes SOC des métriques en temps réel sur le trafic et les comportements du réseau, ainsi que des alertes sur les activités suspectes couplées à des réponses automatisées pour arrêter les activités d'attaque potentielles avant qu'elles ne causent des dommages importants.

# Comment la NDR améliore la défense et la réponse en matière de cybersécurité

Compte tenu des coûts élevés et de la perte de temps opérationnel qu'entraîne une attaque par ransomware, il est impératif de détecter toute activité d'attaque et d'y remédier le plus rapidement possible. Vous ne voudriez pas que votre entreprise fasse partie des 43 % qui ont dû faire le ménage après une attaque par ransomware réussie. Il en va de même pour d'autres méthodes de cyberattaque telles que les différents types de logiciels malveillants, les APT, etc.

La NDR fonctionne en tandem avec le SIEM, l'EDR et d'autres technologies déployées à différents niveaux et emplacements au sein d'une infrastructure de déploiement informatique. La NDR surveille le trafic nord-sud et est-ouest pour mettre en évidence les anomalies du réseau qui indiquent une activité malveillante provenant de menaces externes ou internes indétectables par les outils de sécurité du périmètre et des points d'extrémité. Les meilleurs outils NDR combinent les données de paquets et les données de flux pour une détection plus précise et une aide à la faisabilité du déploiement. Ils peuvent également passer à la capture et à l'analyse de l'ensemble des paquets du réseau lorsqu'un événement anormal se produit. La capture complète des paquets nécessite de grandes quantités de stockage et de puissance de calcul sur les réseaux modernes à large bande passante et ne devrait être utilisée que lorsque l'analyse des données de flux ne permet pas de capturer les données nécessaires.

Une solution de NDR doit proposer les fonctionnalités suivantes pour collaborer avec les autres outils de la triade de visibilité SOC afin d'améliorer la sécurité globale :

## Détection des menaces

L'utilisation conjointe de techniques basées sur des signatures et d'autres techniques non basées sur des signatures permet d'identifier et de mettre en évidence le trafic et l'activité suspects et anormaux du réseau. Une détection rapide est essentielle pour empêcher les attaques de se propager par le biais d'un mouvement latéral des nœuds infectés vers d'autres nœuds, ce qui permet le déplacement de logiciels malveillants et d'autres logiciels d'attaque vers des systèmes


© 2024 Progress. Tous droits réservés.

informatiques compromis. La détection des menaces s'effectue par l'analyse du trafic réseau, et comme les logiciels malveillants ou les réseaux zombies doivent communiquer sur le réseau à un moment ou à un autre pour se propager ou exfiltrer des données, la NDR élimine tous les angles morts de l'infrastructure informatique que d'autres solutions de protection ne voient pas.

## Chasse aux menaces

Les solutions NDR recherchent activement et en temps réel les menaces sur le réseau. Elles recherchent les comportements anormaux, les dispositifs inconnus et d'autres menaces supplémentaires qui représentent un risque. La recherche active de menaces sur le réseau est étroitement liée à la collecte et à la consommation d'informations sur les menaces :

- **Renseignements relatifs aux menaces -** Il existe de nombreux renseignements sur les menaces connues sur l'internet. Les solutions NDR ingèrent ces informations sur les menaces et peuvent les utiliser pour identifier les activités liées à des sites cybercriminels connus et les bloquer sur la base de leur réputation ou d'autres paramètres. Les renseignements sur les menaces proviennent de listes de sources ouvertes fiables, de listes gouvernementales et de fournisseurs commerciaux.

- **Expertise humaine -** De nos jours, il est impossible d'enquêter manuellement sur un volume considérable d'anomalies. L'apprentissage automatique et l'intelligence heuristique permettent de gagner rapidement du temps en ce qui concerne les événements répétitifs et la chasse aux menaces. Il est essentiel de disposer d'analystes expérimentés pour se concentrer sur les événements intéressants. C'est là que l'expertise humaine entre en jeu pour examiner et analyser manuellement les comportements signalés par les algorithmes. Cette combinaison reste le meilleur moyen d'assurer une détection complète des menaces et une réponse appropriée.

## Réponse aux incidents

Les réponses en temps réel aux activités détectées sont essentielles pour minimiser l'impact des attaquants qui contournent les autres mesures de sécurité. Les solutions de NDR peuvent déclencher des mesures de réponse prédéfinies dans d'autres solutions de protection en plus de leur fonctionnalité d'alerte. L'alerte en temps réel, qui permet aux équipes de cybersécurité d'être informées dès que possible de toute activité suspecte détectée, est un élément essentiel de la NDR. Cela doit être fait de manière à réduire les alertes faussement positives, généralement par le biais de l'apprentissage automatique et de procédures algorithmiques avancées d'analyse des menaces.

## Digital Forensics

Les solutions NDR surveillent et stockent des informations sur toute l'activité du réseau entre les nœuds du réseau. Les informations enregistrées sont généralement les adresses réseau des deux nœuds qui communiquent, la durée de leur liaison réseau, les ports utilisés, la quantité de données transmises et les métadonnées extraites de la couche 7. Les informations enregistrées par la NDR n'incluent pas les données transmises entre les systèmes, à moins qu'elles ne soient interceptées explicitement via la capture de paquets en réponse à un événement anormal. Dans la plupart des cas, la solution ADS de Flowmon n'aura pas besoin d'effectuer une capture complète des paquets.

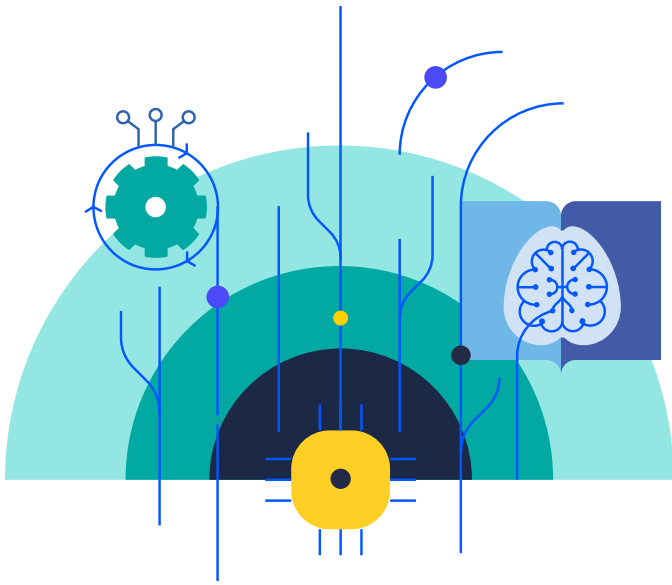

© 2024 Progress. Tous droits réservés.

C'est pourquoi elle est plus flexible, plus facile à mettre à l'échelle et moins chère à déployer et à exploiter qu'une solution NDR qui repose sur la capture de paquets. Les données NDR capturées peuvent être utilisées pour une analyse ultérieure du réseau via des tableaux de bord et des rapports personnalisés. Le service Digital Forensics comprend également des analyses post incident afin d'obtenir une image complète de la manière dont les cybercriminels ont accédé au réseau, de sorte que toute lacune en matière de sécurité puisse être comblée.

Les administrateurs système peuvent déployer les solutions NDR de différentes manières en fonction de l'infrastructure réseau utilisée au sein de l'entreprise. Le déploiement on-premise, dans le Cloud et un mélange hybride des deux est typique, tout comme le déploiement de collecteurs de données basés sur des logiciels à des points stratégiques du réseau pour collecter des données télémétriques à des fins d'analyse.

# Qu'est-ce qui différencie Flowmon ADS des autres systèmes de surveillance réseau ?

Il existe depuis un certain temps des outils qui surveillent le trafic réseau et utilisent des algorithmes statistiques pour mettre en évidence les écarts par rapport au comportement de base. Ces outils fonctionnent bien pour les anomalies significatives qui se manifestent par un volume de trafic important et un écart par rapport à la ligne de base. Les menaces modernes passent sous le radar des algorithmes statistiques et ne sont donc pas détectées. Flowmon ADS marque une évolution de ces outils d'analyse. En effet, Flowmon ADS va au-delà des fonctionnalités traditionnelles et au-delà de l'analyse statistique. Le diagramme ci-dessous illustre l'intelligence supplémentaire que Flowmon ADS ajoute lors de la détection.





© 2024 Progress. Tous droits réservés.

## Machine Learning

Un moteur de détection recourt à diverses techniques d'apprentissage automatique pour détecter les irrégularités suspectes dans le trafic réseau. Le moteur basé sur l'apprentissage automatique peut utiliser l'apprentissage supervisé et non supervisé dans les scénarios de formation pour apprendre l'activité typique du réseau et donc être capable de repérer et d'alerter sur l'activité anormale. Flowmon recourt aux approches d'apprentissage automatique suivantes :

1. **Apprentissage non supervisé -** Grâce à cette technique, Flowmon apprend directement sur le réseau surveillé, sans que les données circulant sur le réseau ne soient marquées ou étiquetées à l'avance. Pour ce faire, les approches suivantes sont utilisées :

- **Prédiction basée sur des données historiques** - Flowmon construit un algorithme de régression linéaire pour ajuster une courbe linéaire aux valeurs des données historiques et, au fil du temps, ajuste les nouvelles données à la courbe et examine comment les choses devraient se présenter en fonction de cette courbe dans l'intervalle de temps suivant. Toute donnée qui sort du modèle mathématique est signalée par une alerte.

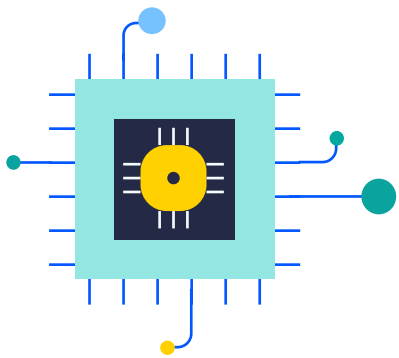
Flowmon utilise également quatre techniques pour détecter les types de données anormaux :

- **Algorithmes de clustering** - Flowmon crée des groupes de données à partir de l'activité des données collectées sur le réseau, qui sont marquées comme des données correctes pour l'activité régulière du réseau. Si une future collecte de données inclut des données qui sortent de cette norme définie, elle est marquée comme une anomalie.

- **Automates probabilistes** - L'état du réseau est modélisé à l'aide d'états et de probabilités de transition en utilisant des données de réseau normales. Les automates algorithmiques de probabilité prennent l'activité du réseau comme entrée pour la comparer aux modèles qui ont été construits. En cas de non-concordance, une anomalie est signalée.

- **Modélisation statistique** - Un modèle statistique du réseau est créé et si l'activité future ne correspond pas à ce modèle, Flowmon la signale comme une anomalie.

- **Modélisation entropique** - Cette méthode est utilisée pour créer une image du réseau, et si cette valeur entropique varie ultérieurement, une anomalie est générée.





© 2024 Progress. Tous droits réservés.

2. **Apprentissage supervisé** - Cette technique utilise des informations connues sur les menaces existantes comme données étiquetées. Par suite, le moteur d'apprentissage automatique de Flowmon s'en sert pour rechercher des menaces connues, des acteurs et des domaines indésirables. L'apprentissage supervisé permet de :

- **Détecter les domaines aléatoires** - le système utilise un modèle de langage probabiliste formé pour reconnaître les domaines Internet légitimes. Si une demande d'accès ou une tentative de connexion provient d'un domaine qui ne correspond pas au modèle, ou si un domaine semble essayer d'imiter un domaine légitime, cela est détecté et des alertes sont alors générées.

- **Détecter l'utilisation de DNS sur HTTPS** - les requêtes DNS cryptées sur HTTPS sont un vecteur d'attaque courant. Un modèle d'apprentissage supervisé utilisant un arbre de décision inspecte le DNS d'entrée sur HTTPS en utilisant des données de comportement historiques dans l'ensemble de formation pour identifier l'utilisation légitime ou l'activité d'attaque possible..

3. **Baselining adaptatif** - À ne pas confondre avec le baselining qui fait partie des outils traditionnels d'analyse du comportement du réseau. L'Adaptive Baselining de Flowmon travaille au niveau de chaque hôte du réseau et apprend comment chaque hôte se comporte généralement par rapport aux autres hôtes avec lesquels il communique. Ainsi, Flowmon peut rapidement repérer un changement soudain de comportement d'un hôte, comme la transmission d'une grande quantité de données, ce qui est souvent le signe d'une copie de données en vue de leur exfiltration vers des serveurs contrôlés par des cybercriminels sur l'internet.

4. **Heuristique** - Les algorithmes heuristiques se concentrent sur un ensemble particulier de comportements afin que les administrateurs système puissent les détecter s'ils se produisent sur un réseau. Par exemple, lorsqu'un utilisateur d'un réseau utilise un client pour communiquer avec un réseau peer-to-peer non approuvé comme BitTorrent, cette activité génère de nombreux symptômes révélateurs qui sont reconnus et évalués à l'aide d'un modèle probabiliste. Les algorithmes heuristiques créés pour repérer des activités spécifiques de ce type permettent de les arrêter presque immédiatement.

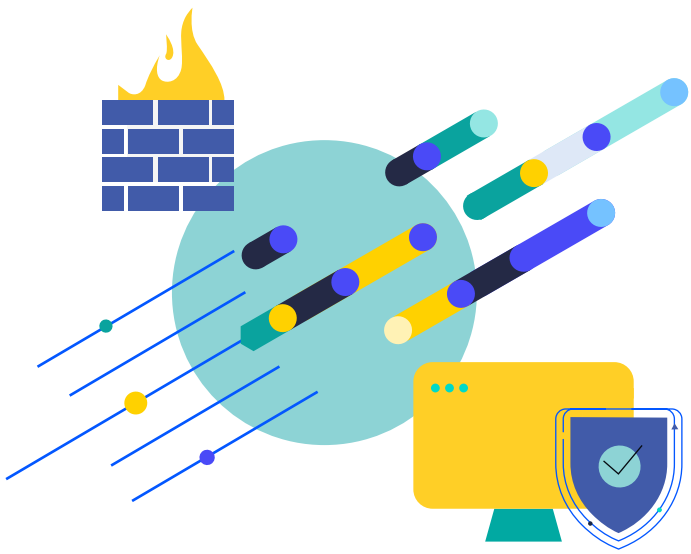
5. **Veille stratégique** - Comme indiqué précédemment, les données de renseignement provenant de diverses sources fiables sont intégrées à l'analyse ADS de Flowmon. Les informations ingérées peuvent provenir de sources ouvertes (telles que MISP), commerciales et gouvernementales et inclure des données sur les IP malveillantes connues, les noms d'hôte, les noms de domaine, l'usurpation de signature de certificat de sécurité, etc. Ces données font partie des renseignements sur les menaces décrits précédemment et peuvent inclure des signatures connues et d'autres données qui mettent en évidence des indicateurs de compromission connus lorsque Flowmon ADS les détecte sur un réseau. En outre, Flowmon ADS intègre la technologie de Suricata pour détecter et mettre en évidence les événements IDS.


© 2024 Progress. Tous droits réservés.

L'ADS (Anomaly Detection System) fait apparaître les alertes et autres informations d'analyse de manière à faciliter la compréhension de la menace détectée. Ce système phare de Flowmon présente en effet une visualisation des incidents riche en contexte, basée sur les catégories du framework MITRE ATT&CK, afin de permettre aux techniciens et aux non-techniciens d'être au courant de la portée, de la gravité et des exigences futures pour répondre aux menaces actuelles, dans un langage qu'ils comprendront. Le fait d'encadrer les alertes et les rapports dans le framework MITRE ATT&CK permet également de comparer de manière cohérente les résultats de plusieurs systèmes de sécurité sur l'image de la sécurité. Cette taxonomie globale des activités des attaquants aide les défenseurs à mieux comprendre le type d'activité que représente une détection particulière.

# La place de la NDR dans la défense globale de la cybersécurité

Logiquement, la NDR s'inscrit dans une stratégie globale de cybersécurité entre les défenses périmétriques et la sécurité des points d'extrémité, comme le montre le diagramme ci-dessous.



En surveillant en permanence toute l'activité du réseau qui passe entre les nœuds du réseau et le trafic entrant et sortant des réseaux privés vers l'Internet, la NDR se positionne comme une source unique de vérité pour l'ensemble du trafic réseau. Associée à la capacité de surveiller et d'analyser même le trafic réseau crypté, la NDR permet de détecter les anomalies en temps réel, d'analyser les menaces et de donner l'alerte. La capacité de la NDR à réagir rapidement aux menaces détectées permet d'arrêter les cyberattaques bien plus tôt que si la NDR n'était pas utilisée.

En permettant cette vision holistique du réseau, combinée à des solutions de sécurité périmétrique, de SIEM et d'EDR, la NDR contribue à améliorer la visibilité et l'observabilité des opérations réseau.


© 2024 Progress. Tous droits réservés.

Le SIEM et l'EDR sont essentiels, mais ils laissent des angles morts qui permettent aux attaquants de dissimuler leur code malveillant après avoir échappé aux défenses périmétriques. De plus, l'EDR ne peut pas être déployé sur tous les appareils du réseau. Par exemple, les appareils IoT constituent souvent un problème de sécurité important, et nombre d'entre eux ne peuvent pas être protégés par l'EDR. En adoptant plutôt une approche basée sur le réseau, la NDR comble ces lacunes critiques en matière de visibilité et de couverture. Les ensembles d'outils combinés portent la défense de la cybersécurité à un tout autre niveau en assurant :

## Observabilité NetSecOps

L'observabilité assure une visibilité exceptionnelle sur le réseau et les applications qui s'y exécutent. Pour les équipes NetSecOps, Flowmon propose la surveillance et le diagnostic des performances réseau (NPMD) pour les NetOps et la NDR pour les SecOps. Cela signifie qu'il n'y a pas de barrières ou de silos de données entre ces groupes, leur permettant ainsi de collaborer depuis un seul point de vue, avec les mêmes données réseau agrégées et de tenir les promesses de NetSecOps. Cela permet aux différents services de fournir un MTTR efficace, de prévenir les incidents de cybersécurité, les pannes et les interruptions, et enfin de réduire les temps d'arrêt et les failles de sécurité.

## Conformité réglementaire

Les entreprises de la plupart des secteurs doivent mettre en œuvre des mesures et des obligations réglementaires et s'y conformer. La surveillance intelligente du réseau, la collecte et l'archivage des données, les alertes et les rapports que Flowmon fournit sont exigés par de nombreux cadres réglementaires.


© 2024 Progress. Tous droits réservés.

Flowmon peut par exemple aider les entreprises à répondre aux exigences réglementaires suivantes :

- **Europe**
  - Directive sur la sécurité des réseaux et des systèmes d'information (NIS2)
  - Directive sur la résilience des entités critiques (RCE)
  - Loi sur la résilience opérationnelle numérique (Loi DORA)

- **USA**
  - Health Insurance Portability and Accountability Act (HIPAA)
  - California Consumer Privacy Act (CCPA)

- **Arabie Saoudite**
  - Contrôles essentiels de cybersécurité (ECC)

En outre, il existe de nombreux autres cadres réglementaires existants et émergents au niveau national et sectoriel (par exemple, PCI DSS dans le secteur financier)..

## Mise en place d'une architecture de sécurité adaptative pour les SOC et les CSIRT

Disposer d'un SOC robuste et d'une équipe d'experts pour le faire fonctionner 24 heures sur 24 et 7 jours sur 7 est essentiel pour mettre en place une bonne stratégie de cybersécurité et une défense au jour le jour. Comme mentionné ci-dessus, les meilleures solutions défensives de cybersécurité combinent l'automatisation intelligente et l'expertise humaine. Flowmon ADS permet aux experts en cybersécurité travaillant dans les équipes CSIRT des SOC d'exploiter une architecture de sécurité adaptative automatisée qui détecte les menaces et les anomalies, identifie celles qui sont faussement positives et met en évidence celles qui doivent être examinées par des experts humains. Il s'agit d'une partie fondamentale du cycle de réponse aux incidents où la détection et l'analyse sont importantes pour le confinement, la découverte et l'éradication, suivies d'activités post-incident avec des capacités approfondies en matière d'analyse numérique des réseaux (Digital Network Forensics). Tout cela permet d'être mieux préparé en ce qui concerne les procédures de traitement des incidents.

© 2024 Progress. Tous droits réservés.

# Le point de vue des analystes sur le marché de la NDR

Comme le montre l'inclusion de la NDR dans la triade de visibilité SOC, les analystes de Gartner considèrent l'utilisation de la NDR comme un élément crucial d'une posture de défense plus large en matière de cybersécurité. Dans son **Market Guide for Network Detection and Response**, Gartner explique :

> *« Le marché de la NDR connaît une croissance régulière et s'étend à de nouveaux cas d'utilisation, tels que l'IaaS. Les responsables de la sécurité et de la gestion des risques doivent donner la priorité à la NDR en tant que complément d'autres outils de détection, en se concentrant sur des taux de faux positifs faibles et sur la détection d'anomalies que les autres outils de contrôle ne couvrent pas. »*

Dans le Quadrant Knowledge Solutions (QKS) **SPARK Matrix™: Network Detection and Response (NDR)**, publié en août 2022, QKS indique :

> *« La technologie de détection et de réponse du réseau (NDR) est née de la nécessité de détecter et d'atténuer les menaces qui peuvent échapper aux solutions de sécurité traditionnelles. Le besoin de telles solutions s'est accéléré à la suite de la pandémie de COVID-19 et de la banalisation du travail à distance qui en a découlé. Ce phénomène se traduit par la connexion de différents dispositifs non sécurisés aux réseaux et points d'extrémité des entreprises, ce qui les rend vulnérables à divers types de cybermenaces, notamment aux logiciels malveillants et aux attaques par ransomware. Les solutions NDR contribuent à atténuer la situation en fournissant aux équipes SOC des entreprises une gestion avancée en temps réel, en exposant les menaces et en réagissant pour les enrayer. »*

Ils proposent également cette définition d'une solution NDR :

> *« C'est une solution qui s'appuie sur des techniques non basées sur les signatures, notamment le Machine Learning (ML) et d'autres techniques analytiques, pour détecter le trafic malveillant et suspect dans le réseau de l'entreprise. Les outils surveillent le réseau et émettent des alertes en cas de trafic suspect. En outre, les solutions NDR fournissent des réponses automatisées et manuelles aux menaces. Ces réponses consistent en des outils de chasse aux menaces et de réponse aux incidents qui ingèrent et mettent en corrélation en permanence de grands volumes de trafic réseau et d'événements de sécurité sur de multiples actifs et points d'accès. »*



© 2024 Progress. Tous droits réservés.

## Évaluation de Flowmon ADS par un analyste

Le rapport QKS Spark Matrix a évalué et présenté les capacités des leaders dans le domaine des solutions NDR. Parmi les 22 solutions de fournisseurs que QKS a incluses dans son rapport, la solution Progress Flowmon ADS a été placée dans le segment des leaders technologiques en raison de ses scores élevés en termes d'impact sur les clients et d'excellence technologique. Pour citer le rapport Spark Matrix :

> *« Progress Flowmon ADS propose une détection complète et une atténuation des cybermenaces sur le réseau de l'utilisateur en ajoutant la couche réseau à la triade de visibilité SOC. Progress Flowmon ADS dispose d'un moteur de détection à base de ML, qui combine plusieurs mécanismes de détection pour révéler les comportements malveillants, les violations de données et les attaques contre les applications critiques du cycle de vie des menaces. Progress Flowmon ADS propose un tableau de bord personnalisé basé sur des règles de sévérité à différents niveaux pour hiérarchiser et signaler les problèmes de sécurité et de réseau. En outre, il permet l'intégration avec le SIEM, les plateformes de big data, le contrôle d'accès au réseau, l'authentification, le pare-feu et d'autres outils de réponse aux incidents tout en ingérant des données provenant de diverses sources telles que AWS, Google Cloud, Progress LoadMaster, et d'autres. »*

Le rapport QKS Spark Matrix est accessible via la section « Références » à la fin de ce livre blanc.

## Ce qu'en disent les utilisateurs de Flowmon

Environ 800 entreprises dans le monde ont adopté la solution ADS de Flowmon pour améliorer leur cybersécurité, leur détection de réseau et leur réponse. Des études de cas et des commentaires d'un grand nombre de ces clients Flowmon sont disponibles sur la page Nos clients (également liée à la section des références ci-dessous). Nous en citons deux et vous encourageons à en consulter d'autres.

Orange résout rapidement de nombreux problèmes pour ses équipes de sécurité et d'opérations réseau en utilisant **Flowmon - Citation de Henrich Snajder (responsable de la sécurité de l'information, Orange Slovaquie**) :

> *« Le service des opérations réseau utilise Flowmon quotidiennement. Ils surveillent le réseau d'ingénierie pour la planification et la capacité afin de voir la structure des différents protocoles dans le réseau. Ils utilisent également des tableaux de bord pour obtenir une visibilité sur les services et les applications du réseau afin de localiser les pannes et de faciliter des réponses plus rapides pour résoudre ces problèmes. »*

**Coop déploie Progress Flowmon pour observer et signaler le trafic de données de ses 1300 filiales** - Roberto Abeledo Alonso, administrateur réseau chez Coop, a déclaré :

*« Nous avons constaté que Flowmon pouvait gérer notre trafic de données et présenter les informations beaucoup plus rapidement que notre solution actuelle, sans oublier la facilité d'utilisation du portail Flowmon, qui était plus facile à utiliser que ce que nous avions auparavant. »*



© 2023 Progress. All Rights Reserved.

# Le point de vue d'un analyste sur le marché de la NDR

Des détails complets sur Flowmon ADS sont disponibles à partir de ce lien et via la section des références. Sur ces pages, vous trouverez des informations détaillées sur la façon dont Progress Flowmon constitue une solution NDR de pointe qui s'adapte aux besoins des PME et des plus grandes entreprises, sans être trop complexe pour les équipes informatiques et de cybersécurité.

De plus, sur notre site web, vous pouvez vous inscrire pour un essai gratuit et entièrement fonctionnel de Flowmon. Si vous souhaitez parler à un expert pour en savoir plus ou obtenir de l'aide pour votre essai, veuillez utiliser notre formulaire de contact.



© 2024 Progress. Tous droits réservés.

# Références

Liens vers les rapports, les pages produits et les sources de données mentionnés dans ce livre blanc.


Progress : Progress nommé leader en matière de détection et de réponse réseau par Quadrant Knowledge Solutions

SPARK Matrix™: Network Detection and Response (NDR), 2022

Sophos: The State of Ransomware 2022

Gartner: Market Guide for Network Detection and Response (Compte requis)

Progress Flowmon : nos clients

Flowmon NDR

Flowmon ADS

Essai gratuit de Flowmon

Formulaire de contact Progress Flowmon


**Demandez votre essai GRATUIT de Flowmon pour 30 jours !**

## À propos de Progress

Progress (Nasdaq : PRGS) propose des logiciels qui permettent aux entreprises de développer et de déployer leurs applications et expériences stratégiques, ainsi que de gérer efficacement leurs plateformes de données, leur Cloud et leur infrastructure informatique. En tant que fournisseur expérimenté et de confiance, nous facilitons la vie des professionnels de la technologie. Plus de 4 millions de développeurs et de technologues dans des centaines de milliers d'entreprises dépendent de Progress. Pour en savoir plus, rendez-vous sur www.progress.com


2024 Progress Software Corporation et/ou ses filiales ou sociétés affiliées. Tous droits réservés. Rev 2024/10 RITM0199651FR


/progresssw
/progresssw
/progresssw
/progress-software
/progress_sw_

Progress