CUSTOMER STORY

CAISSE DES DÉPÔTS

> Disposer d'un partenaire capable d'entendre nos besoins concrets et de nous permettre d'influencer la feuille de route technologique est un avantage stratégique majeur ; nous ne sommes pas un simple numéro, mais un acteur capable de co-évoluer avec l'outil.

Christophe Cavrot, Directeur Sécurité, Architecture et Stratégie Technologique

CDC Informatique - **Groupe Caisse des Dépôts**

#FINANCEPUBLIQUE #PUBLIC #PRIVÉ #NDR #ECONOMIE #VISIBILITÉ

CHRISTOPHE CAVROT_

Directeur Sécurité, Architecture et Stratégie Technologique -

CDC Informatique - Groupe Caisse des Dépôts

01 POUVEZ-VOUS PRÉSENTER LA CAISSE DES DÉPÔTS ET LES MISSIONS QUI DÉFINISSENT VOTRE ACTION ?

La Caisse des Dépôts est un groupe public et un investisseur de long terme. Sa mission fondamentale consiste à servir l'intérêt général et à soutenir le développement économique du pays, en appui des politiques conduites par l'État et les collectivités locales.

L'action du groupe s'articule autour de cinq piliers stratégiques qui touchent le quotidien de millions de Français :

> **La protection de l'épargne populaire :** L'institution garantit la sécurité des dépôts de plus de 50 millions d'épargnants (Livret A, LDDS, LEP). Ces fonds sont ensuite transformés en prêts à très long terme pour financer des projets d'envergure nationale.

> **Le financement du logement social :** En tant que premier financeur du secteur en France, le groupe assure plus de 70 % des besoins de financement pour la création de nouveaux logements sociaux.

> **Un rôle de tiers de confiance :** La Caisse des Dépôts gère des mandats publics et des fonds privés protégés par la loi (fonds des notaires, consignations). Elle assure également un rôle de banquier pour la Sécurité sociale et diverses institutions.

> **L'accompagnement des parcours de vie :** À travers la gestion des retraites et de services numériques gratuits comme Mon Compte Formation ou Mon Parcours Handicap, l'institution est présente aux côtés des citoyens à chaque étape de leur vie. Elle opère également des services spécifiques comme Ciclade.fr (pour la recherche de comptes en déshérence).

> **Le soutien au développement économique :** Via la Banque des Territoires ou Bpifrance, le groupe est un investisseur majeur qui accompagne la croissance des entreprises et des start-ups partout sur le territoire.

*Enjeux cybersécurité_*

Sécuriser
les flux financiers critiques et données sensibles soutenant les missions d'intérêt public

Détecter
les menaces dans des environnements complexes, segmentés et régulés, sans impacter la performance

Optimiser
les opérations du SOC face à l'augmentation du volume d'alertes et à la sophistication des menaces

Se conformer à
des exigences réglementaires et de cybersécurité strictes (RGPD, NIS2, LPM)

Gouverner
un écosystème diversifié d'entités avec différents niveaux de criticité et contraintes de sécurité

> *« L'enjeu n'est plus seulement de protéger les portes d'entrée et les cibles finales, mais de maîtriser tout ce qui circule entre les deux. Le NDR transforme notre réseau en une source d'intelligence active pour neutraliser les attaques dès leurs premiers signes.*

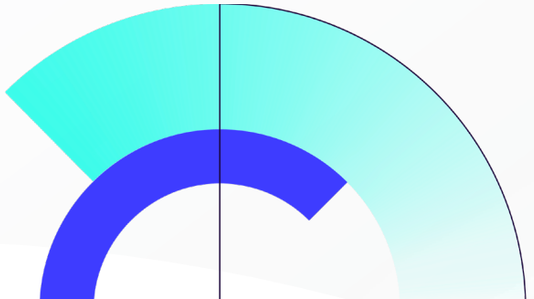
GATEWATCHER

02

AU REGARD DE VOS MISSIONS, QUELS SONT LES PRINCIPAUX ENJEUX DE CYBERSÉCURITÉ AUXQUELS L'ÉTABLISSEMENT DOIT RÉPONDRE ?

Compte tenu de l'hétérogénéité et de la sensibilité des missions de la Caisse des Dépôts, les enjeux de sécurité se cristallisent autour de deux axes majeurs qui s'entremêlent étroitement. D'une part, l'institution doit assurer la protection de l'organisme financier en tant qu'établissement de premier plan, ce qui l'expose à des menaces visant directement ses actifs. L'enjeu est alors de se prémunir contre des tentatives de fraudes classiques ou des attaques sophistiquées cherchant à détourner des fonds ou à manipuler des ordres financiers, le maintien d'un niveau de sécurité robuste étant une condition sine qua non de la confiance institutionnelle.

D'autre part, **la valorisation et la sécurité des données citoyennes constituent une priorité absolue puisque le groupe traite une volumétrie massive d'informations concernant les retraités, les demandeurs de formation ou encore les épargnants français.** Ces données, considérées comme étant de haute qualité en raison de leur caractère actuel et exhaustif, représentent une cible de choix pour des acteurs malveillants souhaitant les revendre ou s'en servir de base pour planifier des cyberattaques plus complexes.



> *« L'intégration de l'intelligence artificielle, et plus particulièrement de l'IA générative, dans la solution Gatewatcher permet d'aller au-delà de la détection classique pour proposer une véritable analyse augmentée, agile et prédictive.*

03

QUELS ÉTAIENT VOS OUTILS EXISTANTS ET COMMENT VOTRE RÉSEAU ÉTAIT-IL SURVEILLÉ ET SÉCURISÉ?

Avant Gatewatcher, notre environnement bénéficiait déjà d'un socle de sécurité classique comprenant la protection des postes et des serveurs, des dispositifs de supervision et de SIEM, ainsi que des solutions dédiées au cloud et au réseau. Ces outils remplissaient leur rôle et permettaient de détecter et de réagir à certaines menaces, mais leur efficacité restait limitée à des incidents déjà déclenchés. Dans la pratique, ils intervenaient souvent trop tard, une fois qu'une attaque avait commencé, et parfois alors même que l'attaquant avait déjà eu accès aux systèmes.

Malgré ces dispositifs, **des angles morts subsistaient**, en particulier sur la **visibilité complète du réseau** et la **détection proactive des comportements anormaux ou malveillants.** Ces lacunes représentaient un risque stratégique : certaines menaces pouvaient évoluer discrètement à l'intérieur de notre infrastructure sans être détectées, mettant en danger la sécurité globale de l'établissement.

SIÈGE SOCIAL
Paris, FRANCE

SECTEUR D'ACTIVITÉ
Principal groupe financier public français, investisseur de long terme, missions d'intérêt public, services financiers pour l'État, les collectivités et les secteurs stratégiques

~350 000 EMPLOYÉS
au sein du Groupe (plusieurs milliers dans les fonctions IT, digitales et sécurité)

PARC INFORMATIQUE
> Plusieurs dizaines de milliers de postes de travail et serveurs
> Systèmes d'information très hétérogènes couvrant les infrastructures critiques, applications financières, flux interbancaires et institutionnels, ainsi que les environnements bureautiques

PÉRIMÈTRE SURVEILLÉ
> Environnement multi-entités et multi-sites, incluant le siège, les data centers, les filiales et les plateformes régulées
> Flux financiers critiques, échanges inter-entreprises, environnements cloud privé et hybrides

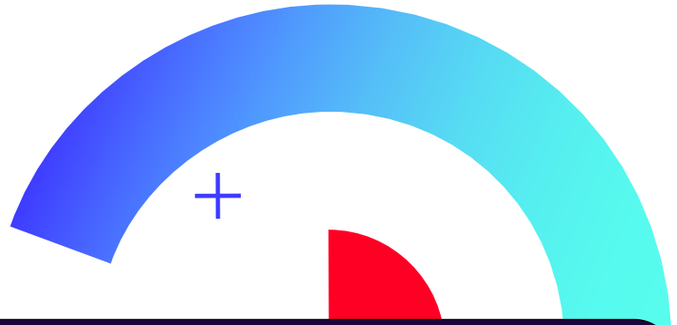
04 QU'EST-CE QUI A FINALEMENT CONVAINCU L'ÉTABLISSEMENT D'ADOPTER UNE PLATEFORME NDR ?

L'analyse de l'existant a mis en lumière un besoin de visibilité accrue, car historiquement, les efforts de sécurisation se concentraient sur deux extrémités bien précises : la périphérie, protégée par les firewalls ou les WAF, et le poste de travail, sécurisé par les EDR et l'antivirus. Cependant, l'espace entre ces deux piliers, c'est-à-dire l'ensemble des flux circulant entre les serveurs, les postes et le périmètre, restait complexe à surveiller avec précision. **Face à des menaces de plus en plus sophistiquées, les outils traditionnels, souvent trop statiques, montraient leurs limites, rendant l'adoption d'une solution de NDR (Network Detection and Response) indispensable** pour répondre à trois attentes stratégiques majeures.

D'abord, il s'agissait de **combler l'angle mort du réseau** en déployant un équipement capable d'analyser les flux de manière dynamique et continue, là où les dispositifs classiques ne permettaient qu'une vision partielle.

Ensuite, cette plateforme devait **faciliter la prise de décision en apportant une meilleure compréhension du trafic interne,** permettant d'identifier des comportements anormaux plus tôt et d'orienter les actions de remédiation de façon beaucoup plus agile.

Enfin, l'objectif fondamental était de **passer d'une réaction subie à une prévention active.** Grâce au NDR, l'institution peut désormais agir en amont : plutôt que d'intervenir une fois que l'attaque a déjà atteint sa cible finale, elle est en mesure de détecter la menace durant son transit et de l'intercepter avant qu'elle ne produise ses effets.



> *« Le véritable avantage, c'est de jouer le coup d'avant plutôt que le coup d'après. Sur un poste de travail ou un serveur, quand une alerte se déclenche, l'attaquant est déjà là et le système est parfois déjà endommagé. Avec l'analyse réseau, le nettoyage se fait en amont, avant même que l'attaque n'atteigne sa cible.*

05 POURQUOI AVOIR CHOISI GATEWATCHER PARMI LES ALTERNATIVES, ET QU'EST-CE QUI A FAIT LA DIFFÉRENCE POUR VOS ÉQUIPES ?

Le choix de Gatewatcher s'est imposé naturellement à l'issue d'un processus d'appel d'offres rigoureux, tant la solution s'inscrit dans l'ADN de la Caisse des Dépôts et sa stratégie de résilience numérique. En tant qu'institution publique, s'appuyer sur un acteur européen doté d'un ancrage français est un argument de souveraineté essentiel qui renforce la confiance dans nos infrastructures. Au-delà de cette dimension politique, c'est la **proximité partenariale** qui a fait la différence par rapport aux géants américains du secteur. **Disposer d'un partenaire capable d'entendre nos besoins concrets et de nous permettre d'influencer la feuille de route technologique est un avantage stratégique majeur ; nous ne sommes pas un simple numéro, mais un acteur capable de co-évoluer avec l'outil.**

Cette confiance est par ailleurs confortée par la **reconnaissance du marché**, notamment celle de **Gartner qui qualifie Gatewatcher de « visionnaire ».** Pour une institution comme la nôtre, qui s'appuie sur ces standards internationaux pour piloter sa stratégie, cette validation est un **gage de crédibilité indispensable.**

Finalement, **l'intégration de l'intelligence artificielle, et plus particulièrement de l'IA générative, dans la solution Gatewatcher permet d'aller au-delà de la détection classique pour proposer une véritable analyse augmentée, agile et prédictive.** Ces travaux sur l'innovation s'encastrent parfaitement dans notre dynamique de SOC nouvelle génération, où la technologie vient soutenir l'expertise humaine pour faire face à l'évolution des menaces.

06

QUELLES SONT LES CAPACITÉS DE LA PLATEFORME QUE VOUS EXPLOITEZ LE PLUS ET COMMENT S'INTÈGRENT-ELLES À VOTRE ÉCOSYSTÈME ?

La force de la solution Gatewatcher réside dans son **exhaustivité,** apportant une **brique d'analyse réseau en profondeur qui complète nos dispositifs existants en couvrant l'intégralité de la chaîne d'intrusion, ou Kill Chain.** Au quotidien, nos équipes exploitent cette capacité pour réaliser une **analyse multi-moteurs** et une inspection des flux **en temps réel** ; outre les moteurs antiviraux locaux qui constituent une première brique de base, nous nous appuyons sur la solution pour l'examen rigoureux des métadonnées. Cette approche nous permet de détecter des signaux faibles et des techniques avancées en surveillant des éléments critiques, tels que les commandes PowerShell circulant sur le réseau, le « beaconing » lié aux serveurs de commande (C2), ou encore les diverses techniques de tunneling.

Cette panoplie de fonctionnalités, particulièrement bien structurée, permet de couvrir toutes les phases d'attaque, de la reconnaissance à l'exfiltration en passant par la persistance. Nous exploitons pour cela des capacités de détection d'anomalies (NBA) et l'identification de domaines malveillants (DGA), incluant la détection de Shellcodes et de ransomwares, qu'ils soient en phase de reconnaissance ou d'exécution. En venant supprimer nos anciens angles morts, l'intégration de Gatewatcher dans notre écosystème justifie une approche stratégique fondamentale : agir directement sur le flux plutôt que d'attendre l'impact sur l'hôte.

Le véritable avantage, c'est de jouer le coup d'avant plutôt que le coup d'après. Sur un poste de travail ou un serveur, quand une alerte se déclenche, l'attaquant est déjà là et le système est parfois déjà endommagé. Avec l'analyse réseau, le nettoyage se fait en amont, avant même que l'attaque n'atteigne sa cible.

> *« L'analyste augmenté, c'est celui qui peut se concentrer sur l'expertise et la valeur ajoutée. En confiant le traitement automatique du bruit à l'intelligence artificielle de la plateforme, nous diminuons la fatigue opérationnelle et augmentons notre réactivité sur les menaces réelles.*

07

COMMENT S'EST DÉROULÉ LE DÉPLOIEMENT DE LA SOLUTION ET QUELS ENSEIGNEMENTS TIREZ-VOUS DE CETTE PHASE DE MISE EN ŒUVRE ?

Le déploiement de la solution s'est déroulé de manière particulièrement fluide, suivant un calendrier maîtrisé malgré un démarrage en période estivale.

On peut distinguer deux grandes phases structurantes : d'abord, une mise en service technique rapide de deux mois qui a englobé l'ensemble de la chaîne, de la commande à l'installation physique des équipements. Une fois les machines en place, l'activation proprement dite a été extrêmement véloce, permettant d'obtenir les premiers rapports d'analyse exploitables en quelques jours seulement. S'en est suivie **une phase d'optimisation ciblée** de quatre mois où, plutôt que de subir un flux massif d'alertes dès l'allumage, l'approche a consisté à prioriser les fonctionnalités. La granularité de la plateforme a ainsi permis de réaliser un **tuning progressif**, isolant d'abord les fonctions sans faux positifs avant d'affiner les analyses réseau plus complexes.

Cette phase d'implémentation a également apporté des enseignements majeurs et une valeur ajoutée inattendue en termes d'hygiène du système d'information. **Ce que l'on pouvait initialement prendre pour des faux positifs lors du réglage s'est révélé être un excellent outil d'audit, mettant en lumière des serveurs qui généraient des flux anormaux ou illégitimes.** Grâce à cette visibilité assainie et granulaire, l'institution a pu mener un véritable travail de nettoyage réseau en corrigeant des configurations de serveurs qui, sans l'apport du NDR, seraient restées dans l'ombre. Cette étape a transformé une simple installation technique en une opération de salubrité numérique indispensable.

L'un des grands bénéfices de cette phase a été la capacité de l'outil à faire émerger des comportements réseau anormaux sur nos propres serveurs. Ce n'était pas seulement une phase de configuration, c'était une véritable opération de nettoyage et d'assainissement de notre système d'information.

08

QUELS RÉSULTATS CONCRETS OBSERVEZ-VOUS AUJOURD'HUI EN TERMES DE RÉACTIVITÉ ET DE GESTION DE VOS OPÉRATIONS DE SÉCURITÉ ?

L'intégration de Gatewatcher a permis de franchir une étape décisive vers ce que l'on appelle le « SOC augmenté », un concept dont les bénéfices se mesurent sur trois piliers essentiels pour l'efficacité de notre cyberdéfense.

Le premier enjeu, et l'un des plus importants, est **la lutte contre la fatigue des analystes.** Les équipes de niveau 1 passent souvent un temps considérable sur des actions répétitives qui génèrent une lassitude inévitable et, par extension, un risque d'erreur humaine . En automatisant le traitement d'une grande partie des alertes à faible valeur ajoutée, la solution parvient à gommer le bruit de fond du système d'information.

Ce gain d'efficacité permet un second pilier stratégique : **le recentrage sur les missions à haute valeur ajoutée.** En libérant les analystes de ces tâches routinières, nous leur redonnons du temps pour ce qui nécessite réellement leur expertise, comme l'investigation approfondie, la prise de décision et le tuning de la sécurité. Ce temps précieux est ainsi réinvesti dans la création de nouvelles alertes pour anticiper les menaces émergentes plutôt que de simplement les subir.

Enfin, cette transformation repose sur **une vision d'investigation consolidée** qui faisait défaut jusqu'alors. Si nous disposions auparavant des logs de l'EDR sur les postes et des flux firewall, il nous manquait le détail fin de ce qui transitait réellement sur le réseau. Aujourd'hui, l'analyse réseau vient corréler l'ensemble de ces informations, offrant une vision globale du processus d'attaque qui apporte une vraie sérénité aux équipes. Elles disposent désormais d'une compréhension complète et détaillée de la chaîne d'intrusion, permettant une réponse plus juste et plus rapide.

L'analyste augmenté, c'est celui qui peut se concentrer sur l'expertise et la valeur ajoutée. En confiant le traitement automatique du bruit à l'intelligence artificielle de la plateforme, nous diminuons la fatigue opérationnelle et augmentons notre réactivité sur les menaces réelles.

09

POUVEZ-VOUS PARTAGER UN EXEMPLE MARQUANT OÙ LA PLATEFORME NDR A ÉVITÉ UN INCIDENT OU AMÉLIORÉ LA QUALITÉ DE SERVICE CHEZ UN CLIENT ?

Plus que l'évitement d'un incident isolé, l'apport de la plateforme réside dans un véritable changement de posture sur l'analyse. **Le NDR a permis de combler ce que l'on pourrait appeler le « chaînon manquant » de notre visibilité.**

Aujourd'hui, cet outil nous permet d'anticiper les alertes et d'obtenir une vision complète de l'incident. Là où nous devions auparavant jongler entre les flux firewall et les données de l'EDR sans lien direct, nous disposons désormais d'une analyse fine des flux qui arrivent sur les serveurs ou les postes de travail. **Cette corrélation nous donne une compréhension totale du processus d'attaque.**

L'autre bénéfice marquant, que nous avons évoqué, **concerne l'évolution vers un « SOC augmenté ».** L'outil apprend de notre environnement, ce qui est une réelle avancée grâce à l'IA. Cela permet de réduire la fatigue des analystes en automatisant le traitement du bruit de fond, pour nous concentrer sur les alertes à forte valeur ajoutée.

Enfin, cette solution nous accompagne **dans le respect de nos exigences réglementaires** les plus strictes, qu'il s'agisse de DORA, du RGPD ou des réglementations bancaires et de la Loi Pacte. C'est un pilier de notre stratégie pour sécuriser l'ensemble de nos métiers : Banque des Territoires, politiques sociales, gestion d'actifs et participations stratégiques.

Bénéfices clés de la plateforme NDR_

Visibilité complète et non-intrusive
sur tous les flux (N/S & E/O), y compris chiffrés

Détection comportementale
renforcée et enrichie par IA

Priorisation intelligente et contextualisation
des alertes

Intégration fluide
avec l'écosystème SOC existant

Cloisonnement par entité
et supervision unifiée

Réduction du MTTD et du MTTR
grâce à l'automatisation

Mise en conformité facilitée
sans perte de performance opérationnelle

Aide à la prise de décision

GATEWATCHER

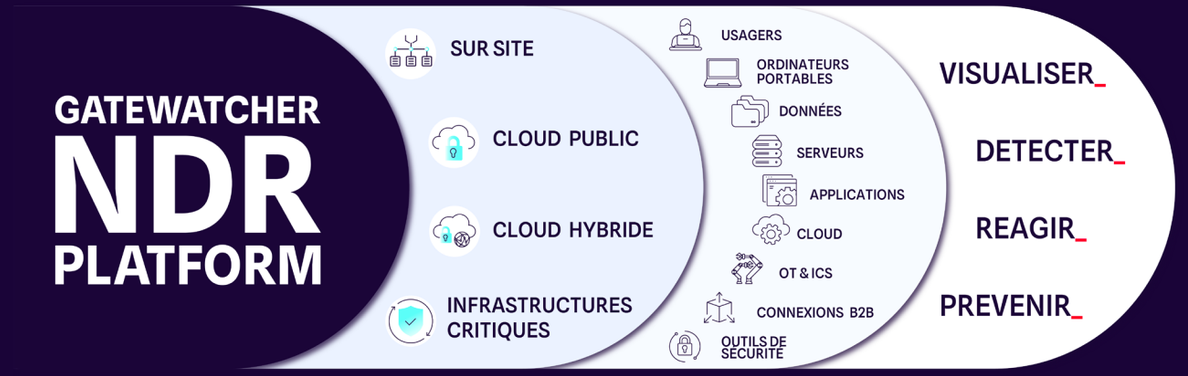
CAISSE DES DÉPÔTS

*À propos_*

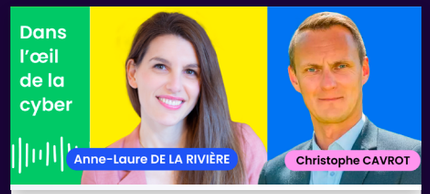
Leader de la détection des cybermenaces, Gatewatcher protège depuis 2015 les réseaux des entreprises et des institutions publiques, y compris les plus critiques. La plateforme NDR Gatewatcher (Network Detection and Response), combine intelligence artificielle et techniques d'analyse dynamiques et comportementales contextualisées. Elle offre ainsi une visibilité unifiée et complète, une détection et une cartographie des systèmes en temps réel et une réponse autonome, automatisée et priorisée face aux attaques grâce à l'IA agentique. Déployée sur infrastructures cloud, on-premise ou sensibles, et compatible avec les environnements IT, OT et IoT, elle sécurise l'ensemble des actifs critiques et simplifie les opérations grâce à son assistant IA intégré. Gatewatcher allie puissance technologique et sérénité opérationnelle, afin d'aligner la cybersécurité sur vos objectifs business.

Gatewatcher a été reconnu comme Visionary dans le 2025 Gartner® Magic Quadrant™ for Network Detection and Response (NDR).

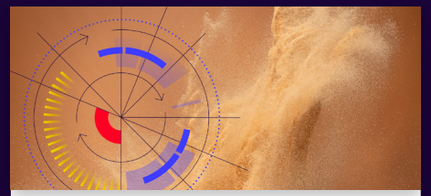
Contactez-nous



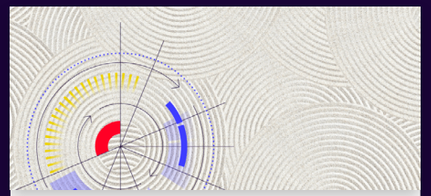
Envie d'en *savoir plus ?_*



[PODCAST]
Au cœur de la finance publique : quand la cybersécurité soutient l'économie



[USE CASE]
Augmenter l'efficacité du SOC



[USE CASE]
Améliorer votre temps de réponse (MTTR) aux incidents de sécurité