CUSTOMER STORY

BANQUE D'INVESTISSEMENT_

"Le NDR est devenu notre filet à mailles fines : il capte ce que les autres solutions laissent passer. Dans un environnement où une seconde de latence peut coûter des millions, cette visibilité est vitale.

Directeur cybersécurité d'une banque de financement et d'investissement

#BANQUEINVESTISSEMENT #CYBERRESILIENCE #NDR

> *Au-delà des données clients, ce sont nos algorithmes de trading, nos plateformes transactionnelles et nos flux temps réel qu'il faut protéger.*

01

POUVEZ-VOUS PRÉSENTER VOTRE ORGANISATION ET LES ENJEUX DE CYBERSÉCURITÉ SPÉCIFIQUES AU SECTEUR DE LA BANQUE D'INVESTISSEMENT ?

Nous sommes un groupe bancaire majeur opérant sur les activités de marchés, de gestion d'actifs et de banque privée. Dans ce contexte, notre exposition aux menaces cyber est constante et évolutive. Nous faisons face à des attaques ciblées, souvent sophistiquées, mêlant phishing ciblé, mouvements latéraux discrets ou exploitation de chaînes d'attaque complexes. Le fait d'être interconnectés avec des places de marché, des contreparties internationales, des infrastructures critiques comme SWIFT, accroît fortement le risque systémique. **Au-delà des données clients, ce sont nos algorithmes de trading, nos plateformes transactionnelles et nos flux temps réel qu'il faut protéger.** Nous devons concilier cela avec un haut niveau d'**exigence réglementaire** (PCI DSS, DORA, EBA, RGPD, etc.) sans jamais impacter notre **performance opérationnelle.** Notre mission est de garantir que la cybersécurité n'est jamais un frein à la stratégie d'investissement.

02

QUELS ÉTAIENT VOS OBJECTIFS EN MATIÈRE DE CYBERSÉCURITÉ AVANT LE DÉPLOIEMENT DU NDR ?

Notre priorité était d'accroître notre visibilité sur les segments critiques du réseau, notamment les flux interbancaires, les environnements de trading ou encore les couches d'authentification sensibles. Nous souhaitions **détecter plus en amont** les comportements anormaux, **même lorsque les flux sont chiffrés ou cloisonnés.** Les solutions EDR ou SIEM ne nous suffisaient plus : trop de bruit, des angles morts, et une charge trop importante pour nos équipes. Il nous fallait une solution passive mais exhaustive, **capable de remonter des signaux faibles sans impacter les opérations.** Enfin, nous avions **besoin d'automatiser certaines réponses simples, tout en conservant la main sur les décisions critiques**.

*Enjeux cybersécurité_*

Protéger
les flux critiques interbancaires et les données transactionnelles sensibles.

Surveiller
les environnements segmentés et chiffrés sans impacter la performance.

Réduire
la charge opérationnelle du SOC face à l'augmentation et la disparité des alertes.

Répondre
aux exigences réglementaires (DORA, PCI DSS, NIS2).

Superviser
des entités multiples avec des niveaux de criticité différents.

03

POURQUOI AVOIR OPTÉ POUR UNE APPROCHE NDR ET QUELLES LACUNES CETTE TECHNOLOGIE VENAIT-ELLE COMBLER ?

La technologie NDR est venue compléter notre architecture XDR existante. Contrairement à l'EDR qui se limite aux endpoints, le NDR analyse l'ensemble des flux réseau, y compris entre systèmes ou vers l'extérieur. Dans un environnement sensible, cette capacité à détecter les mouvements latéraux, les scans internes ou les comportements déviants est essentielle. Nous avons d'abord déployé la sonde de détection **Gatewatcher TRACKWATCH** sur nos segments les plus sensibles, notamment ceux liés aux systèmes de paiement, en raison de sa qualification par l'ANSSI et son respect des exigences à la LPM. En parallèle, nous avons choisi **la plateforme NDR de Gatewatcher** pour étendre cette visibilité sur nos environnements non sensibles (bureautique, imprimantes, RH, etc.), tout en gardant une supervision unifiée. **Cette dualité nous permet de traiter chaque zone selon son niveau de criticité tout en gardant une vision transverse.**

04

QUELS CRITÈRES ONT MOTIVÉ LE CHOIX DE GATEWATCHER PARMI D'AUTRES SOLUTIONS ?

Outre l'aspect souverain, qui reste un prérequis pour nos environnements critiques, ce qui nous a véritablement convaincus chez Gatewatcher, c'est la richesse de son **moteur de détection multivectorielle,** alliée à une interface à la fois lisible et maniable. La plateforme permet une lecture immédiate des alertes, tout en offrant la possibilité d'**investiguer** en profondeur lorsque le contexte l'exige. Ce double niveau de lecture, entre **simplicité d'usage et puissance analytique**, correspond parfaitement à nos exigences opérationnelles. L'interface de management intuitive, nous a séduits pour la **gestion multi-entités**, un besoin clé dans un groupe où chaque filiale dispose de son propre périmètre.

Enfin, Reflex nous a permis d'orchestrer des **scénarios de remédiation simples, interopérables avec nos équipements déjà installés.** La plateforme NDR a su s'intégrer à notre stack existant sans ajouter de complexité inutile. Enfin, Trackwatch étant qualifié ANSSI, il répondait pleinement à nos **obligations réglementaires** pour les environnements sensibles. Cette certification s'accompagne d'un **durcissement complet de la solution** à tous les niveaux, matériel, système, applicatif, garantissant l'intégrité, la confidentialité et la résilience face aux menaces, y compris de type zero-day. Ce niveau de sécurisation nous apporte une sérénité essentielle dans des contextes aussi critiques.

SIEGE SOCIAL
PARIS
FRANCE

SECTEUR D'ACTIVITÉ
Banque d'investissement, marchés de capitaux, financement structuré, services pour grandes entreprises

EFFECTIFS ESTIMÉS / TAILLE
~ 10 000 à 15 000 collaborateurs dédiés aux lignes "investment & markets" (hors banque de détail)

PÉRIMÈTRE SUPERVISÉ
Plus de 20 sites incluant sièges, datacenters, salles de marchés et plateformes critiques. Réseaux segmentés, hybrides, incluant des interconnexions SWIFT, SEPA, cloud privé et zones réglementées.

PARC INFORMATIQUE
Environ 20000 postes et serveurs, avec supervision des SI métiers, systèmes de paiement, flux interbancaires et environnements bureautiques.

L'approche non-intrusive de Gatewatcher a permis un déploiement sans coupure ni impact sur les applications sensibles.

05

COMMENT S'EST DÉROULÉE L'INTÉGRATION DE LA SOLUTION DANS VOTRE ENVIRONNEMENT COMPLEXE ?

L'intégration s'est faite en plusieurs phases. Nous avons commencé par les environnements critiques, avec des appliances physiques déployés dans nos zones sensibles. L'approche non-intrusive de Gatewatcher a permis un **déploiement sans coupure ni impact sur les applications sensibles.** La plateforme propose deux modes distincts : un **déploiement on-premise**, indispensable pour les segments soumis à des contraintes réglementaires fortes, **et une version cloud,** plus adaptée aux environnements administratifs ou hybrides. Cette flexibilité nous a permis d'ajuster le dispositif à la cartographie de nos risques. Les connecteurs natifs nous ont permis d'interfacer rapidement la plateforme avec nos SIEM, et autres solutions. Dès les premières semaines, nous avons observé une nette amélioration de la visibilité réseau et une baisse de notre temps de réaction. **L'accompagnement de Gatewatcher a été structurant : tuning des règles, création de playbooks, coaching de nos analystes SOC… Cela a grandement facilité l'adoption et la configuration.**

06

QUELS BÉNÉFICES CONCRETS AVEZ-VOUS OBSERVÉS DEPUIS LA MISE EN PLACE DE LA SOLUTION ?

Nous avons **significativement réduit notre temps de détection et notre temps de remédiation.** Là où il nous fallait auparavant plusieurs heures pour qualifier une alerte, aujourd'hui, quelques minutes suffisent. **La détection comportementale nous a permis d'identifier des tentatives de reconnaissance réseau qui seraient passées sous les radars des autres outils.** Le NDR nous offre une supervision globale, avec un cloisonnement précis pour chaque entité du groupe. **La charge cognitive pour les analystes a diminué grâce au triage intelligent des alertes.** J'ajoute que la capacité à déclencher des actions automatisées nous fait gagner un temps précieux sur des incidents récurrents. Nos analystes peuvent désormais se focaliser sur ce qui importe vraiment et **sont en contrôle des décisions.**

07

QUELLE PLACE OCCUPE LE NDR DANS VOTRE STRATÉGIE DE GOUVERNANCE CYBER ?

Le NDR n'est pas un outil isolé : c'est une brique stratégique de notre gouvernance cyber. Il nous apporte des métriques précises sur le comportement réseau, les anomalies, les surfaces d'exposition. **Ces indicateurs alimentent nos comités de pilotage et influencent nos arbitrages.** Le fait de disposer d'une **plateforme souveraine, segmentable par entité, mais pilotable de façon centrale** est fondamental pour nous. Cela nous permet de fédérer des politiques de sécurité tout en laissant une certaine autonomie locale. **Le NDR nous aide aussi à valoriser notre démarche sécurité auprès de la direction générale, en rendant les risques visibles, mesurables, et compréhensibles.**

*Les bénéfices du 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

08

COMMENT ASSUREZ-VOUS LA RÉACTIVITÉ FACE À UNE MENACE IDENTIFIÉE ?

Nous combinons plusieurs leviers : la détection avancée en temps réel grâce à la plateforme NDR de Gatewatcher couplée à l'enrichissement contextuel par la CTI, ainsi que des scénarios de réponse automatisés.
Par exemple, en cas de détection d'un scan interne suspect sur un segment bureautique, un playbook est automatiquement déclenché : isolement du poste, notification au SOC, et ticketing automatisé vers l'équipe concernée. Tout cela se fait sans intervention humaine immédiate, mais avec un contrôle à posteriori. Cette approche nous permet d'être très réactifs, tout en gardant la main. **Nous avons ainsi sécurisé plusieurs vecteurs d'attaque potentiels sans impacter nos SLAs.**

09

QUELS SONT VOS PROCHAINS ENJEUX CYBER ET COMMENT GATEWATCHER VOUS Y PRÉPARE ?

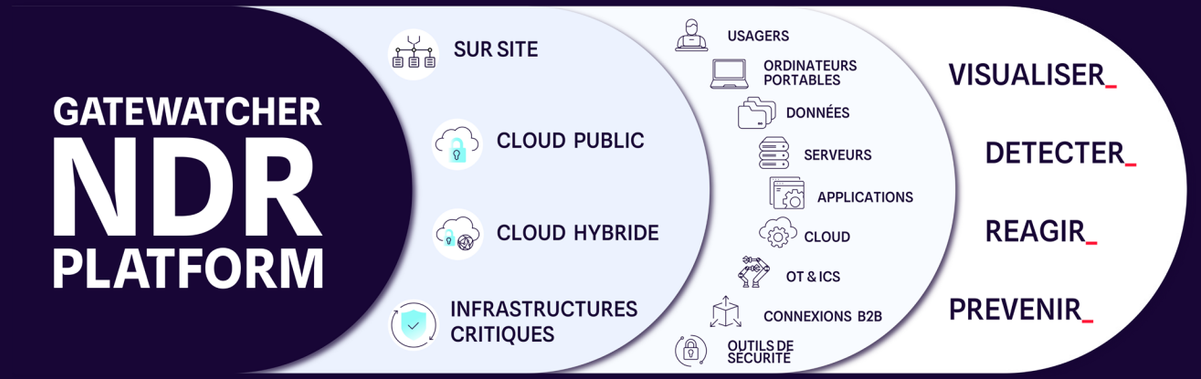
Nous prévoyons une extension progressive de la supervision à d'autres périmètres : reste du cloud, certains environnements offshores, autres entités du groupe. Le modèle décentralisé mais orchestré du NDR est un atout : chaque filiale dispose de sa propre vision, tandis que nous gardons une vue consolidée. Nous travaillons aussi à **renforcer la réponse automatisée,** notamment sur les incidents récurrents, grâce à de nouveaux playbooks.

*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. Grâce à l'association de l'IA à des techniques d'analyse dynamiques, la plateforme NDR de Gatewatcher assiste la prise de décision du SOC par une analyse contextualisée et un triage des alertes. Elle permet une réponse autonome et adaptée à chaque menace identifiée en offrant une visibilité totale sur l'activité du réseau, dans le cloud et on premise. Compatible avec les environnements IT, OT et IoT, elle sécurise l'ensemble des actifs critiques et simplifie les opérations. Gatewatcher allie puissance technologique et sérénité opérationnelle, afin d'aligner la cybersécurité sur vos objectifs business.

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

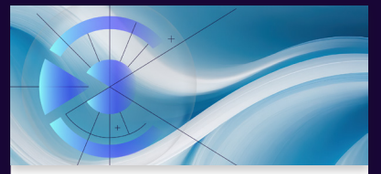
Contactez-nous



Envie d'en *savoir plus* sur le sujet ?_

[PODCAST S4 • E02]
Au cœur de la finance publique : quand la cybersécurité soutient l'économie.

[GUIDE]
Découvrez notre dernier guide NDR.



[CAS D'USAGE]
Améliorer mon temps de détection (MTTD).