CUSTOMER STORY

RENFORCER LA CYBERSÉCURITÉ DANS LE SECTEUR DE LA GRANDE DISTRIBUTION ALIMENTAIRE ET DE LA RESTAURATION_

“

Assurer la sécurité des données de nos clients est non négociable. Avec Gatewatcher, nous pouvons protéger ce qui compte le plus sans faire de compromis sur le service.

#CHAÎNEAPPROVISIONNEMENT #EXPÉRIENCECLIENT #NDR #GRANDEDISTRIBUTION

> *Une violation n'aurait pas seulement des conséquences financières — elle endommagerait gravement la confiance et la réputation de la marque.*

01 QUELS SONT LES DÉFIS SPÉCIFIQUES ET UNIQUES EN MATIÈRE DE CYBERSÉCURITÉ AUXQUELS SONT CONFRONTÉES LES CHAÎNES NATIONALES DE GRANDE DISTRIBUTION ALIMENTAIRE ?

La cybersécurité dans la grande distribution alimentaire s'étend bien au-delà des transactions aux points de vente. Notre organisation gère des milliers de dossiers personnels, de transactions financières et une infrastructure numérique complexe qui couvre tout, des systèmes de point de vente aux plateformes de gestion de la chaîne d'approvisionnement. Avec un écosystème aussi fragmenté, sécuriser chaque point d'entrée représente un défi majeur.

Protéger les clients et les données financières est une priorité absolue. Nos systèmes de commande en ligne, programmes de fidélité et plateformes de vente de distribution traitent d'énormes quantités d'informations personnelles et de détails de paiement, ce qui en fait une cible pour les cybercriminels. Une violation n'aurait pas seulement des conséquences financières — elle endommagerait gravement la confiance et la réputation de la marque.

Au-delà des risques numériques, nos systèmes de gestion des stocks, réseaux de fournisseurs tiers et infrastructure numérique distribuée ajoutent une complexité supplémentaire. Qu'il s'agisse de sécuriser l'accès au réseau des restaurants, de prévenir les intrusions non autorisées ou d'assurer la conformité aux réglementations de sécurité alimentaire et de protection des données, nous devons constamment nous adapter aux menaces évolutives pour maintenir nos opérations sécurisées.

Enjeux cybersécurité _

Contrôler
des écosystèmes numériques fragmentés nécessitant une couverture globale et consolidée à travers les systèmes de point de vente, la gestion des stocks, les chaînes d'approvisionnement et les programmes de fidélité.

Gérer
l'intégration de divers systèmes connectés, y compris les appareils IoT, les applications mobiles et la convergence IT/OT, de manière sécurisée.

Atténuer
les risques liés aux fournisseurs tiers, aux réseaux de vendeurs et aux vulnérabilités dans la chaîne d'approvisionnement.

Assurer
la continuité des opérations pendant les périodes de forte affluence, comme les vacances ou les week-ends, tout en protégeant le suivi de la sécurité alimentaire et la résilience opérationnelle.

Protéger
les données sensibles des clients, les dossiers financiers et la propriété intellectuelle contre les cybercriminels et les accès non autorisés.

02

COMMENT LES PÉRIODES DE FORTE ACTIVITÉ AUGMENTENT-ELLES LES RISQUES DE CYBERSÉCURITÉ ?

Les périodes de forte affluence comme les vacances entraînent une augmentation du trafic numérique et un risque accru de cybermenaces. Avec des millions de commandes en ligne traitées dans des centaines de sites, **notre réseau doit prendre en charge des systèmes de paiement sécurisés, le suivi des stocks et la gestion des données clients,** tout en restant résilient face aux attaques potentielles. Imaginez des systèmes de suivi des stocks défaillants pendant une période d'achat intense— chaînes d'approvisionnement perturbées, perte de revenus et insatisfaction des clients.

Une cyberattaque sur la gestion des stocks et des commandes en temps réel pourrait perturber les opérations, compromettre le suivi de la sécurité alimentaire et éroder la confiance des clients. La portée nationale et de plus en plus mondiale de nos opérations de vente fait de nous une cible encore plus importante. Les cybercriminels peuvent tenter d'interférer avec les communications de la chaîne d'approvisionnement, de surcharger notre infrastructure numérique ou d'exploiter des vulnérabilités dans les systèmes de paiement et de commande.

La grande **diversité des dispositifs de point de vente,** des applications mobiles et des systèmes connectés ajoute au défi, augmentant **le risque d'accès non autorisé ou de violations de données.**

Chaque emplacement de restaurant, chaque plateforme de livraison et chaque point de contact numérique représente **une vulnérabilité potentielle de sécurité qui doit être continuellement surveillée et protégée.**

03

COMMENT NOTRE ARCHITECTURE RÉSEAU EST-ELLE STRUCTURÉE, ET COMMENT LA SOLUTION NDR A-T-ELLE ÉTÉ DÉPLOYÉE ?

Notre organisation exploite un **réseau segmenté, garantissant que les opérations de vente de distribution et les systèmes administratifs restent séparés**. Le réseau de vente de distribution prend en charge les systèmes de point de vente, la gestion des stocks et les plateformes destinées aux clients, tandis que le réseau du siège social gère les transactions financières, les communications internes et la gestion d'entreprise. Cette séparation est essentielle, car les environnements administratifs sont plus vulnérables aux cybermenaces en raison de facteurs humains.

Lors du déploiement de notre NDR (Network Detection and Response), notre priorité était d'**assurer la visibilité dans les deux environnements sans ajouter de complexité.** Nous avons choisi l'**option cloud de la solution** car elle correspondait mieux à nos besoins. Elle a directement fourni une surveillance centralisée du trafic sans interférer avec les opérations quotidiennes. Cette approche, s'appuyant sur notre infrastructure virtualisée, a rendu **le déploiement et l'intégration dans notre cadre de sécurité existant simples** tout en permettant une évolutivité facile. Elle a permis une surveillance en temps réel des deux réseaux, assurant **une détection et une réponse efficaces aux menaces.**

SECTEUR D'ACTIVITÉ
Chaîne régionale de grande distribution alimentaire et de la restauration

REVENUS
> 1,5 milliard £

LOCALISATION
450 points de vente à travers l'Angleterre, l'Écosse, le Pays de Galles et l'Irlande du Nord

ENVIRONNEMENTS DIVERSIFIÉS
Services drive, cuisines centrales mutualisées, systèmes de commande en ligne, applications de livraison, etc

EXPOSITION MONDIALE
> Ingrédients provenant de plus de 15 pays
> Logistique internationale
> Données clients pour les programmes de fidélité mondiaux

04

QU'EST-CE QUI VOUS A CONDUIT À METTRE EN ŒUVRE UNE SOLUTION NDR, ET COMMENT S'INTÈGRE-T-ELLE AUX OUTILS DE SÉCURITÉ EXISTANTS ?

Lorsque nous avons évalué notre paysage de cybersécurité, nous avons réalisé que **le réseau était notre plus grand angle mort.** Nous avions une protection des terminaux **(EDR) couvrant les appareils des utilisateurs et XDR sécurisant les serveurs et les applications,** mais l'activité du réseau restait largement invisible. Sans moyen de détecter les anomalies en temps réel, **nous étions vulnérables aux menaces cachées** se déplaçant de manière non détectée à travers notre infrastructure.

Soyons transparents, **le coût était également un facteur important dans notre décision.** De nombreuses solutions NDR ont un prix élevé, reflétant souvent la reconnaissance de la marque plutôt que la fonctionnalité.

En explorant diverses solutions NDR, ce qui s'est démarqué était l'agilité et l'adaptabilité de Gatewatcher. Au lieu de nous forcer dans un cadre prédéfini, **ils étaient disposés à évoluer avec nous,** aidant à résoudre des vulnérabilités spécifiques à mesure qu'elles apparaissaient. Pour nous, la priorité était de trouver une solution qui offrait une valeur réelle. Alors que certains concurrents se tournaient vers des fournisseurs établis, **nous avons vu un leader émergent avec de solides capacités.**

Pour une entreprise de distribution alimentaire et de boissons, la sécurité doit être rapide, transparente et adaptée à notre environnement unique. La solution NDR **s'intègre parfaitement à notre pile de sécurité existante,** améliorant la visibilité sans perturber les opérations quotidiennes.

05

QUELS ÉTAIENT LES PRINCIPAUX INDICATEURS COMMERCIAUX ET OPÉRATIONNELS QUE VOUS VISIEZ À AMÉLIORER LORS DE L'ÉVALUATION DES SOLUTIONS NDR COMME GATEWATCHER ?

Lorsque nous avons évalué les technologies de détection et réponse réseau, **Gatewatcher est apparu comme une solution innovante** qui a fondamentalement repensé notre approche de la cybersécurité. Notre objectif principal était la visibilité — pas seulement une surveillance passive, mais **des informations intelligentes et contextuelles qui pouvaient faire la différence entre le bruit et les menaces réelles.**

Les outils de sécurité ne sont efficaces que s'ils fournissent des informations claires et exploitables — sinon, ils génèrent trop de bruit, submergeant les équipes avec de faux positifs.

L'écosystème technologique fragmenté de la grande distribution alimentaire et de la restauration crée des défis uniques en matière de cybersécurité. La plateforme NDR de Gatewatcher détecte également des menaces dissimulées **(Shadow IT)** — où les unités opérationnelles mettent en œuvre des solutions technologiques non autorisées en dehors de la gouvernance informatique centralisée.

> *Notre objectif principal était la visibilité – pas seulement une surveillance passive, mais des informations intelligentes et contextuelles qui pouvaient faire la différence entre le bruit et les menaces réelles.*

Dans notre industrie, cela se manifeste par des scénarios critiques : centres de distribution avec des systèmes d'inventaire indépendants, emplacements de franchise utilisant des solutions de point de vente personnalisées, et équipes marketing déployant des plateformes de collecte de données non autorisées. **Ces improvisations technologiques créent des vulnérabilités de sécurité potentielles que les approches de surveillance traditionnelles ne peuvent pas détecter.**

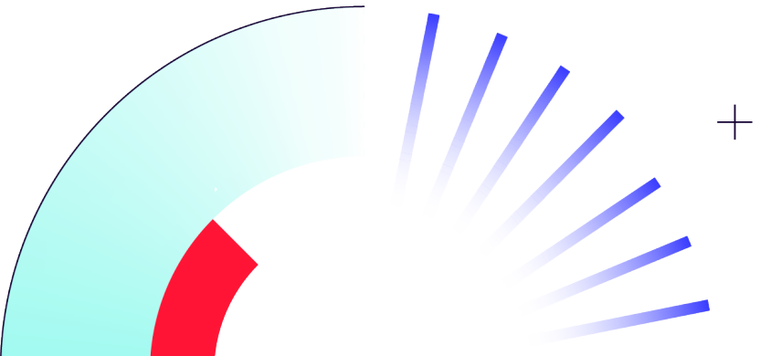
En **cartographiant les actifs** et **en surveillant les communications** à travers les environnements IT et OT, elle découvre des points de terminaison technologiques cachés. La plateforme transforme le Shadow IT d'une faiblesse potentielle en un écosystème gérable et transparent, fournissant une visibilité en temps réel sur les interactions technologiques, des systèmes de stockage frigorifique aux plateformes de commerce électronique.

06

COMMENT AVEZ-VOUS INTÉGRÉ GATEWATCHER DANS VOTRE STRATÉGIE XDR (EXTENDED DETECTION AND RESPONSE) ?

Gatewatcher est devenu la pierre angulaire de notre stratégie XDR, reliant des domaines de sécurité critiques avec une sophistication sans précédent. **Là où les solutions traditionnelles créent des silos de sécurité fragmentés, la technologie de Gatewatcher crée un écosystème de sécurité unifié et intelligent qui corrèle les données à travers les terminaux, les environnements cloud et les infrastructures réseau.**

La capacité de la solution à s'intégrer parfaitement à **nos outils de sécurité existants tout en fournissant une vue centralisée** et complète de notre paysage numérique est tout simplement révolutionnaire. Gatewatcher **ne comble pas seulement les lacunes de sécurité** — il transforme **notre façon de conceptualiser et de mettre en œuvre la cybersécurité dans un paysage numérique en rapide évolution.**



07

COMMENT GATEWATCHER S'ALIGNE-T-IL AVEC VOS OBJECTIFS STRATÉGIQUES DE SÉCURITÉ ?

La solution NDR de Gatewatcher a transcendé les paradigmes traditionnels de sécurité en offrant une approche holistique de la protection du réseau. Leur technologie ne se contente pas de détecter les menaces — elle les interprète dans le contexte complexe de notre paysage opérationnel. En intégrant **une analyse avancée basée sur l'IA,** Gatewatcher fournit **un niveau d'intelligence sur les menaces qui transforme notre sécurité d'une défense réactive à un mécanisme d'intelligence proactive.**

Ce qui a distingué Gatewatcher était leur engagement à créer une solution qui communique avec notre environnement spécifique. Leur NDR ne se contente pas de surveiller ; **il analyse et cartographie en temps réel les flux de communication complexes entre nos systèmes** de gestion de la chaîne d'approvisionnement, nos plateformes de point de vente et notre infrastructure d'entreprise.

Gatewatcher sécurise les systèmes de point de vente et les données clients, permettant aux acteurs du retail de faire face aux cybermenaces **sans compromettre l'efficacité ou la qualité de service.**

> *Nous n'optimisons pas seulement notre infrastructure de sécurité pour répondre aux besoins opérationnels d'aujourd'hui, mais nous nous préparons aussi de manière proactive aux risques de demain.*

08

COMMENT CELA POSE-T-IL LES BASES POUR L'AVENIR ?

Alors que notre industrie continue d'évoluer, ce partenariat jette des bases solides pour l'innovation future en matière de cybersécurité. **Les solutions modulaires et flexibles de Gatewatcher** nous positionnent pour faire face aux menaces émergentes tout en maintenant l'adaptabilité nécessaire pour relever les défis dynamiques du secteur de la distribution alimentaire et de la restauration.

En adoptant une culture d'amélioration continue, nous n'optimisons pas seulement notre infrastructure de sécurité pour répondre aux besoins opérationnels d'aujourd'hui, mais nous nous préparons aussi de manière proactive aux risques de demain.

Avec les technologies avancées de détection réseau de Gatewatcher, nous avons la confiance nécessaire pour protéger nos opérations de vente, préserver la confiance des clients et assurer la sécurité **et la résilience à long terme de notre industrie.**

GATEWATCHER

Gatewatcher sécurise les systèmes de point de vente et les données clients, permettant aux distributeurs de faire face aux cybermenaces sans sacrifier l'efficacité ou le service. Nous sommes fiers de soutenir une industrie construite sur la confiance et la résilience.

*Vos avantages_*

La technologie Gatewatcher permet de :

Sécuriser un écosystème distribué et fragmenté
Fournit une surveillance en temps réel à travers les magasins, les chaînes d'approvisionnement et les plateformes en ligne.

Gérer les périodes de forte demande
Détecte et neutralise les menaces y compris durant les pics de ventes, les vacances et les événements à forte affluence.

Contrôler les pics d'exposition
Suit et analyse les appareils connectés et les interactions réseau en magasin et en ligne.

Améliorer la visibilité sur les menaces
Identifie les attaques exploitant les vulnérabilités dans les systèmes de paiement, les données clients et la gestion des stocks.

Corréler efficacement les signaux de sécurité
Unifie les alertes à travers les systèmes informatiques et opérationnels pour une détection rapide des menaces, y compris sur trafic chiffré.

Réduire les perturbations opérationnelles
S'adapte facilement (plug-and detect) et sans aucun impact sur vos activités : implémentation rapide, passive et sans agent.

Flexibilité de la solution
La technologie NDR peut être utilisée sur site ou dans le cloud, selon le niveau de sensibilité des entités à protéger ou votre architecture existante.

Plateforme **NDR_**
GATEWATCHER

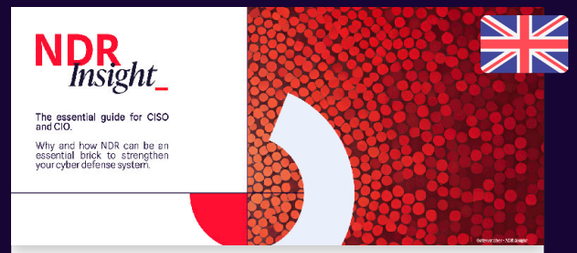
GEN AI_
CTI_
NDR_
DEEP VISIBILITY_
TAP_

La plateforme NDR de Gatewatcher offre une cartographie des cybermenaces et une analyse comportementale afin d'assurer la détection des attaques ciblées, même en cas de flux de données chiffrées. Elle combine notamment du machine learning avec des analyses statiques et dynamiques.

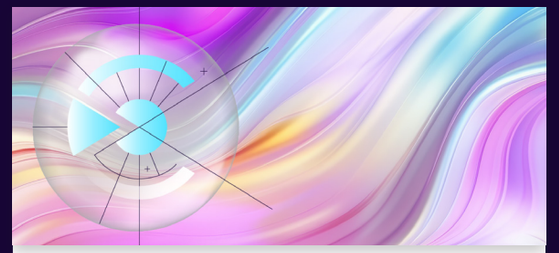
GATEWATCHER

Envie d'en *savoir plus ?*_

[VIDEO]
Easy as NDR:
Le R de NDR, qu'est ce que c'est ?



[GUIDE]
Découvrez notre dernier guide NDR Insight.



[CAS D'USAGE]
Se prémunir des attaques par supply chain

*Easy as*_

NDR_ CTI_ TAP_ GEN AI_ DEEP VISIBILITY_

Contactez-nous