Construire un avenir plus sûr dans le commerce de détail

kaspersky PRÊTS POUR L'AVENIR

https://go.kaspersky.com/Retail-fr.html

2021

Introduction

Si vous êtes un leader dans le domaine du commerce de détail, vous êtes forcément un héros.

Aucune industrie sur la planète n'a utilisé la technologie de manière aussi efficace et n'a pris autant le contrôle et les commandes sur son destin que le secteur du commerce de détail. Aucune.

Non seulement vous l'**avez fait**, mais vous l'avez fait à votre image.

Les conditions étaient loin d'être idéales, que ce soit pour les salariés ou les entreprises. Le commerce de détail se positionne à côté des secteurs de l'accueil et du voyage, qui ont été lourdement affectés par les restrictions de santé publique.

Cependant, nous pensons qu'il est temps de tourner le dos à l'examen de nos blessures et d'essayer de recoller les morceaux de ce qui nous est arrivé.

Tout le monde parle toujours de la manière dont nous avons été « forcés » à évoluer et à nous transformer. Nous n'allons pas faire cela dans ce document. Pas seulement parce que ce sont des clichés, mais parce que cela part du principe que les détaillants sont en position de passivité, victimes des circonstances. Ce n'est pas ce que nous constatons lorsque nous examinons la manière dont ce secteur a utilisé la technologie pour se transformer.

Nous avons la même approche par rapport au terme de « nouvelle norme ». Si les experts de la vente au détail pensent que la « norme » n'a jamais été « nouvelle » avant 2019, c'est qu'ils n'ont pas été très attentifs. Et d'ailleurs, nous ne sommes pas intéressés par la « norme », mais par l'élan.

Êtes-vous prêt ?

Ce type de questions est compliqué. Prêt pour quoi ? Comment pouvez-vous être prêt pour un futur qu'on peut difficilement délimiter ?

La plupart des analystes vont déclarer que l'industrie du commerce de détail était déjà prête à mettre en œuvre les technologies qui l'ont aidée à surmonter la vague de la pandémie. La différence résidait dans la longueur de la feuille de route. « Cinq ans de transformation numérique, condensés sur 5 semaines » est une formulation courante.

Mais qui peut dire que cette réduction (d'un marathon à un sprint) a conduit à un résultat inférieur aux délais plus lents prévus par les équipes dirigeantes dans la vente au détail dans le monde ? Désolé pour cette banalité, mais **la nécessité est mère de l'invention**. L'évolution n'est-elle pas un raccourci de la définition même des méthodologies Agile et Lean ?

Faites-le, tout simplement

Ces trois mots ont aidé Nike à faire passer ses parts de marché dans l'Amérique du Nord de 18 % à 43 % entre 1988 et 1998. Ce n'est pas simplement un bon candidat pour le slogan le plus efficace de tous les temps, c'est également un excellent conseil. C'est également la recommandation qu'a suivie l'industrie du commerce de détail depuis le tout début de la pandémie.

Le fait que vous ayez dû réaliser 5 ans de transformation numérique en 5 semaines devrait être célébré, pas simplement parce que vous l'avez effectué, mais parce que cela s'est opéré de la manière la plus difficile, la plus vive et la plus concentrée possible. Cela a conduit, nous le pensons, à un résultat beaucoup plus positif et efficace.

Dans ce document, vous trouverez un compte rendu des tendances essentielles de la technologie vers lesquelles les revendeurs au détail vont se tourner dans les 5 prochaines secondes jusque dans les 5 ans à venir (ou le font déjà probablement). Nous ne sortons ici rien d'un chapeau : tout est basé sur les meilleures recherches de l'industrie disponibles. Si nous en parlons ici, c'est que cela est pertinent. Il ne s'agit pas de science-fiction ni de spéculation, et nous ferons tout notre possible pour éviter un battage médiatique (même si cela est enthousiasmant).

Pour chaque nouvelle tendance technique que nous célébrons, nous allons examiner comment vous pouvez l'utiliser en toute sécurité. Nous sommes en 2021 et nous ne pensons pas que quiconque (personne, entreprise ou secteur) doive hésiter pour adopter des technologies essentielles en raison de préoccupations de sécurité. C'est notre métier.

Gestion de l'inventaire en magasin

Transformation de la chaîne d'approvisionnement numérique

Réalité mixte

Paiements

Analyse du commerce de détail – IA et algorithmes

Marketing agile

Tendance n° 1 : Gestion de l'inventaire en magasin

La gestion de l'inventaire en magasin est un élément nouveau du rapport Gartner Hype Cycle pour 2021, avec une évaluation des avantages de la « transformation » et de la percée se situant entre 5 % et 20 %. Avec la pandémie qui a stimulé de manière tellement impressionnante le taux de croissance des achats en ligne, la gestion de l'inventaire en magasin est essentielle pour les revendeurs au détail, afin de les aider à atteindre leurs objectifs d'activité principaux, notamment :

- Satisfaire la demande où qu'elle soit (incluant la vente sur le trottoir et les achats en ligne avec récupération en magasin)
- Réduire les effets de l'inventaire sur le coût des marchandises vendues
- Tirer parti des données en temps réel afin de prendre des décisions de planification plus avisées
- Réduire le coût de réalisation du commerce en ligne
- Réduire la charge d'inventaire excessive
- Améliorer l'efficacité des employés en magasin et dans l'entrepôt
- Se donner les moyens d'effectuer un véritable commerce unifié pour relier la « brique » au « clic »

Lorsque nous parlons de la gestion d'inventaire en magasin, cela ne concerne pas seulement la technologie. Il s'agit d'un écosystème complexe de technologies, qui intègre l'IoT, les rayons intelligents, le commerce unifié, le paiement intelligent, la planification algorithmique, l'autonomie de la chaîne d'approvisionnement, les centres de micro-exécution, etc.

La meilleure façon de résumer la gestion d'inventaire en magasin (et ses effets) consiste peut-être à se concentrer sur la valeur de la « précision en temps réel ». Sans cela, le commerce unifié (par exemple) est impossible : le mieux que vous pouvez espérer est un secteur avec deux lieux différents, l'un en ligne et l'autre en magasin, chacun essayant désespérément (et échouant) de se connecter à l'autre.

Certaines estimations laissent entendre que la précision d'un inventaire en magasin traditionnel ne dépasse pas 70 %. Cela peut fonctionner lorsque votre activité se compose uniquement de « briques », mais n'est pas adapté aux « clics », et certainement pas aux autres attentes des clients, tels que les achats en ligne avec récupération en magasin.

Comment utiliser la gestion d'inventaire en magasin en toute sécurité ?

Afin de tirer parti d'un retour sur investissement optimal de votre adoption de la gestion d'inventaire en magasin, vous allez devoir partager des données sensibles avec votre fournisseur. Après les données clients, vos données d'inventaire sont la priorité absolue, qui doit bénéficier d'un traitement prudent. Une attaque serait susceptible de révéler vos niveaux de stocks, vos performances de vente, l'emplacement de votre stock et tous les plans que vous pourriez avoir élaborés pour les saisons à venir. Les risques sont encore amplifiés si vous intégrez à la fonctionnalité de gestion d'inventaire en magasin les données clients dans le but d'effectuer des suggestions personnalisées, pour des raisons évidentes. L'attaque sophistiquée aux dépens de DSW (Designer Shoe Warehouse) en 2020 prouve à quel point il est essentiel que les détaillants utilisent la technologie de gestion d'inventaire en magasin en toute sécurité. Au cours d'une attaque par ransomware de l'un des fournisseurs de DSW, le PDG de l'entreprise de vente au détail a indiqué que sa société « avait perdu une partie de ses capacités de ventes numériques pendant deux semaines pendant la saison de ventes déterminante de septembre ».

Suggestions :

- Commander des audits de sécurité réguliers ou choisir un fournisseur de cybersécurité qui inclut cela dans le cadre de son offre.
- Adopter la devise du Mois de la sensibilisation à la cybersécurité en 2020 du NIST : « Si vous connectez l'informatique, protégez l'informatique ». Bien que votre fournisseur de gestion d'inventaire en magasin puisse détenir et traiter vos données sensibles, les capteurs IoT que vous utilisez pour gérer votre inventaire se trouvent dans vos locaux et sont sous votre contrôle. Assurez-vous que vous avez accès à la fonctionnalité de cybersécurité compatible avec l'IoT.
- Acceptez le fait que les attaques sur des fournisseurs tiers sont une certitude, et prévoyez la possibilité que votre fournisseur de gestion de l'inventaire en magasin soit attaqué, en vous assurant de disposer d'un système de réponse aux incidents strict sur place.

Tendance n° 2 : Transformation de la chaîne d'approvisionnement numérique

Selon Gartner, « pratiquement tous les détaillants prévoient d'investir pour rendre leurs chaînes d'approvisionnement plus agiles (96 %) et plus résilientes (90 %) d'ici 2022 ». Cela n'est pas surprenant : le modèle de chaîne d'approvisionnement traditionnel n'est plus approprié.

La pandémie n'est pas le seul facteur ayant encouragé les détaillants à se concentrer sur la transformation de la chaîne d'approvisionnement numérique. Le besoin d'alternatives plus flexibles, légères, réactives et intégrées par rapport aux anciens modèles était déjà clair. delete

Réussir la transformation de la chaîne d'approvisionnement numérique nécessite l'élaboration d'un écosystème sur mesure de plates-formes et de fournisseurs tiers, afin de satisfaire les besoins uniques de votre activité de commerce de détail. Bien que de nombreux détaillants soient déterminés à développer une chaîne d'approvisionnement autonome, ce n'est pas quelque chose qui peut s'effectuer avec une technologie exclusivement propriétaire en interne. Ce recours à un écosystème de fournisseurs ne se cantonne pas à la chaîne d'approvisionnement, et n'est certainement pas l'exclusivité du secteur du commerce de détail. Cependant, comme dans toutes les situations dans lesquelles nous dépendons d'une partie externe pour répondre à nos besoins, cela signifie que nous devons envisager minutieusement ces relations.

BlueYonder, leader selon Gartner dans les systèmes de gestion d'entrepôts, a son slogan sur cette question : « Réalisez votre potentiel », promettant une chaîne d'approvisionnement « automatisée, organisée, intelligente et prédictive ».

Quelques précisions à propos d'un mot : rupture

Rupture. Dites-le à voix haute. Écoutez-vous le dire.

Qu'est-ce que cela signifie pour vous en°2021 ? Qu'est-ce que cela signifiait en 2019 ?

Votre train n'arrive pas à cause d'une rupture de service. La rupture est pénible.

La totalité de votre activité a dû s'arrêter pendant des mois à cause de la rupture due à la pandémie. La rupture est dévastatrice.

Mais qu'en est-il de l'autre côté de la rupture, celui qui a fait bondir de plus en plus loin votre activité vers l'avenir, bien avant 2021 ?

Rupture technologique. Nous vivons pour cela. En laissant de côté la pandémie, aucune des technologies auxquelles votre activité de vente au détail faisait appel avant 2020 n'aurait été possible sans rupture :

- Personnalisation : du marketing aux produits
- Technologie vocale : « Alexa, achète-moi mon papier toilette ! » (Plus facile à dire qu'à faire en mars 2020)
- IA : des chatbots à l'analyse
- Mobile : d'abord les achats, puis les paiements
- IoT : Chaîne d'approvisionnement, analyse des vidéos, inventaire en direct

Tous les éléments de la liste ci-dessus ont dû bouleverser les technologies et les processus existants afin de tenir leurs promesses. C'est la même chose pour la rupture.

Ainsi, lorsque nous parlons de la rupture amenée par la pandémie mondiale, nous devons nous concentrer sur les révolutions dévastatrices qui ont apporté dans le passé des revenus et des efficacités auparavant irréalisables dans le secteur du commerce de détail. Il ne s'agit en aucune façon de minimiser la manière particulière endurée par le secteur du commerce de détail en raison de confinements apparemment sans fin. Pas du tout.

Mais nous avons le choix. Allons-nous nous approprier cette rupture et célébrer l'impulsion inexorable donnée au secteur du commerce de détail ? Ou allons-nous nous polariser sur ses éléments chaotiques ?

Comment utiliser la technologie de chaîne d'approvisionnement numérique en toute sécurité

Les transformations numériques font de chaque organisation une entreprise de logiciels qui dépend d'une multitude de fournisseurs externes, qui viennent s'ajouter à des menaces de tiers difficiles à gérer. Cela peut sembler catégorique, mais lorsqu'il s'agit de cybersécurité, c'est une réalité. Très peu de détaillants (le cas échéant) vont se trouver en position de développer leurs propres écosystèmes privés, et ils vont devoir se tourner vers des fournisseurs extérieurs afin de tirer parti de la technologie dont ils auront besoin pour prospérer à l'avenir. Toutefois, l'adoption de celle-ci n'est que la première étape : ce sont les détaillants qui auront pris les mesures supplémentaires nécessaires pour s'assurer qu'ils utilisent en toute sécurité la technologie de la chaîne d'approvisionnement numérique qui seront les vrais vainqueurs sur le long terme.

Suggestions :

- Établir une politique de gestion des risques liés aux fournisseurs et intégrer des évaluations de risques dans le cadre de vos processus d'acquisition de logiciels tiers.
- Utiliser une solution de cybersécurité qui automatise les analyses des vulnérabilités et les mises à jour correctives, et s'assurer que votre fournisseur est toujours au courant des éventuelles vulnérabilités « zero-day ».
- Faire une priorité de la visibilité des données : si des données sensibles (notamment les données de vos clients) se trouvent dans les mains de l'un de vos fournisseurs tiers, vous devez le savoir.
- Si vous utilisez une quelconque infrastructure de cloud hybride (et, il faut bien l'admettre, qui ne le fait pas ?), vous allez devoir comprendre les limites du modèle de sécurité de la « responsabilité partagée ». Même si votre fournisseur de services cloud partage la responsabilité pour les données qu'il stocke, votre priorité absolue doit toujours être vos propres données, et votre propre résultat financier.

Tendance n° 3 : Réalité mixte

Les critiques ne sont peut-être pas convaincus par le nouveau film Space Jam, mais le fait de regarder LeBron James se métamorphoser en personnage de jeu vidéo est une bonne manière de comprendre les effets de la réalité mixte. C'est également une preuve que la percée de la réalité mixte s'étend bien au-delà du secteur du commerce de détail, et qu'il s'agit d'une expérience de plus en plus attendue par les consommateurs. Vos clients ne sont pas seulement à l'aise avec la réalité mixte, ils l'utilisent couramment.

La fusion entre la réalité augmentée, la réalité virtuelle et le monde réel, incarnée dans Space Jam 2, est la preuve que la réalité mixte est désormais un autre exemple d'une technologie qui était déjà inévitable pour les détaillants, mais dont l'adoption a considérablement été accélérée par la pandémie.

Toutefois, les situations du marché pendant la pandémie signifient que la réalité mixte ne se limite pas à émerveiller les clients avec une expérience. Tout comme les paiements sans contact, la réalité mixte offre également une opportunité pour une interaction sans se toucher, ce qui est désormais un impératif absolu. Et ce n'est pas tout. La réalité mixte donne aux détaillants la possibilité de :

- Augmenter les ventes et les taux de conversion
- Réduire les taux de retour (voir « essayage » ci-dessous)
- Établir des relations avec les clients, grâce à des suggestions personnalisées
- Mieux adapter les produits (parfois littéralement, en repérant les discordances de taille, par exemple)

Pour le commerce de détail, le cas d'utilisation principal de la réalité mixte réside bien sûr dans les technologies d'essai virtuel, telles que celles proposées par des plates-formes comme 3DLOOK. Et une fois encore, la concrétisation de la promesse de la réalité mixte signifie que les détaillants doivent pour cela aussi faire des choix avisés en ce qui concerne les fournisseurs de technologie tiers avec lesquels ils collaborent.

Comment utiliser la réalité mixte en toute sécurité

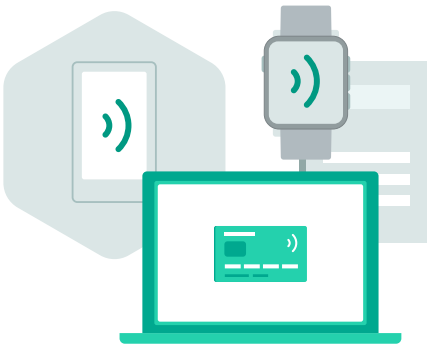
Réalité mixte : surmonter le défi de l'« essayage »

La nouvelle cabine d'essayage se trouve à domicile, si l'on se fie au comportement du consommateur. L'essayage est devenu la pratique courante pour « commander en excès », avec l'intention de retourner tous les éléments qui ne correspondent pas ou qui ne conviennent pas. C'est très bien pour les consommateurs, mais moins bien pour les détaillants, qui doivent supporter les coûts des retours. En outre, en ce qui concerne les retours, la croissance du modèle « Achat en ligne, retour en magasin » est un exemple flagrant de la nécessité de fournir une expérience de commerce unifiée entre la « brique » et le « clic ».

Plus l'expérience de réalité virtuelle est immersive, plus il est urgent pour les entreprises d'utiliser la technologie de manière sécurisée. Lorsqu'il s'agit de réalité mixte, il est facile de voir pourquoi cela est important : après tout, vous demandez à vos clients de télécharger leurs propres visage, corps ou pieds vers une plate-forme en laquelle ils ont confiance, afin de faire interagir cette imagerie privée avec les images de vos produits. La plate-forme à laquelle ils font confiance est la vôtre : le fait que ce soit un tiers qui fournisse la technologie ne fera aucune différence pour vos clients en cas de faille. L'un des risques évidents qui découlent d'une application non sécurisée de la réalité mixte est la colère des régulateurs, mais la situation est plus complexe que cela. Tout d'abord, cela va sans dire que les réglementations varient d'une région à l'autre, de sorte qu'il est important d'être conforme aux environnements de vos consommateurs, où qu'ils se trouvent. Toutefois, la réalité en ce qui concerne les réglementations relatives aux technologies est qu'elles ne sont pas toujours en mesure de maintenir le rythme rapide du développement, ce qui oblige les entreprises à regarder au-delà de la simple conformité, afin de fournir un service de réalité mixte sécurisé dans lequel les consommateurs peuvent avoir confiance.

Suggestions :

- Tenez compte des exigences **éthiques** de vos consommateurs, parallèlement à la conformité réglementaire. Ne vous cantonnez pas à l'option d'une sécurité minimale viable, comme dans un exercice consistant à cocher des cases, mais utilisez plutôt « la ceinture et les bretelles », et indiquez clairement à vos clients que vous faites des efforts supplémentaires pour les protéger.
- N'oubliez pas que vous clients vont utiliser la fonctionnalité de réalité mixte **sur leurs propres appareils**, qui se situent en dehors de votre périmètre informatique et sont susceptibles d'être victimes d'une atteinte physique. Choisissez un fournisseur de cybersécurité disposant d'une Threat Intelligence spécifique à l'industrie et à la région, et qui possède la capacité complète de surveiller votre activité contre les menaces nouvelles et inconnues.
- Faites de la **transparence** votre mot d'ordre en matière de réalité mixte : vous devez savoir exactement ce qui se passe en permanence avec les données de vos clients et, à leurs yeux, c'est **votre** réputation qui est en jeu, pas celle du fournisseur de la technologie de réalité mixte.



Tendance n 4 : Paiements

Ayant déjà transformé en réussite les paiements sans contact (voir ci-dessous), les détaillants et les régulateurs font des efforts considérables pour tirer parti de cette (et d'autres) technologie de paiement pour faire traverser au secteur la situation pandémique.

Les nouvelles frontières sont les suivantes :

- Appareils de points de vente mobiles (avec un taux de croissance annuelle composé prévu de 18 % entre 2021 et 2027)
- Crédit de la part de tiers, comme Klarna
- Plus de caissiers
- Biométrie
- Jetons
- Plates-formes de paiements tierces, telles que PayPal

Là encore, une transformation effective des paiements numériques amène nécessairement les détaillants au contact d'une vaste gamme de fournisseurs de technologies tiers. Dans le cas des paiements (plutôt que, disons, la réalité mixte), ce partenariat avec des fournisseurs tiers ne correspond pas simplement à un besoin technologique. C'est également une nécessité commerciale, la seule manière d'éliminer les frictions et les abandons au moment du paiement.

Le message des consommateurs est clair : « nous sommes en 2021, je ne devrais pas avoir à sortir ma carte de crédit pour acheter quelque chose ! » En adoptant de façon prudente des fournisseurs de paiement tiers, les détaillants ont un parcours clair pour faciliter autant que possible la réalisation de l'achat une fois qu'ils voient la ligne d'arrivée.

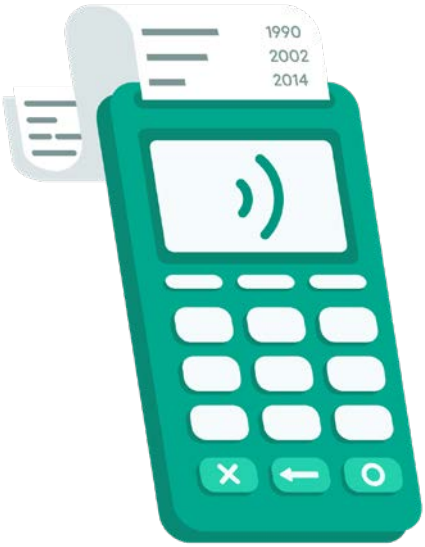
Ne me touchez pas ! Comment les paiements au détail étaient déjà indéniablement prêts pour la distanciation sociale

L'industrie du commerce de détail était **déjà** prête pour de nombreuses situations apportées par la pandémie. Prenons le cas des paiements sans contact dans les magasins.

Cette technologie a tout l'air d'avoir été **conçue pour la distanciation sociale**. Une technologie qui nous permet de jouer un rôle dans nos vies de consommateurs et de détaillants sans toucher l'appareil de point de vente. Et, pour dire les choses simplement, ces appareils peuvent être (comme l'a estimé le Daily Mail), « aussi sales que des toilettes publiques ».

La technologie sans contact aurait pu être développée pour la vitesse, ou pour éviter tout froissement avec les consommateurs (mémorisation des codes PIN, avoir à balayer et signer). Personne n'aurait imaginé en 2014 (date du lancement d'Apple Pay) que le paiement sans contact deviendrait la technologie remarquable de distanciation sociale permettant de lutter contre la pandémie qu'elle s'est avérée être quelques années plus tard.

Les revendeurs, ainsi que les régulateurs gouvernementaux, ont immédiatement tiré parti du paiement sans contact lorsque la pandémie a débuté. Le Royaume-Uni a augmenté la limite des paiements de 30 à 40 livres en avril 2020 (juste après le début du confinement du pays le 23 mars). Un mois plus tard, les paiements sans contact au Royaume-Uni avaient augmenté de 44 %. Une augmentation supplémentaire est fixée pour le 15 octobre, avec une limite de 100 livres.



Un bref historique des paiements sans contact

Cette technologie est disponible depuis les années 90, principalement pour des cas d'utilisation et des commerçants spécifiques (les stations d'essence, par exemple). L'élaboration en commun des normes NFC entre Phillips et Sony en 2002 a ouvert des perspectives urgentes pour une adoption entre secteurs et internationale.

Cela a conduit à tout un cortège d'étapes essentielles dans des régions diverses et des marchés variés, et prouvé l'utilité de la technologie, ainsi que la demande pour celle-ci.

Pour localiser le point de basculement mondial en matière de paiements sans contact, nous devons probablement nous tourner vers 2014 : la naissance d'ApplePay avec l'iPhone 6.

À l'heure actuelle, Google Pay est disponible dans 40 pays et Apple Pay dans 50. Mais il ne s'agit là que d'un début : les portables (et d'autres appareils) vont suivre, pour étendre la libéralisation du mécanisme de paiement de la carte au téléphone et au-delà.

Les paiements sans contact prouvent que le secteur de la vente au détail est plus que prêt pour la montée en puissance de la transformation numérique qui est en train de s'opérer. Plus près que quiconque en dehors de ce secteur (ou de ses leaders informatiques) ne peut l'imaginer.

Comment utiliser la nouvelle technologie de paiements en toute sécurité

Pas plus tard que le 30 septembre 2021, des chercheurs ont découvert une vulnérabilité extrêmement grave de l'iPhone qui autorisait la réalisation de paiements EMV (Europay, Mastercard et Visa), et l'ouverture d'une brèche dans les limites du montant du sans contact (jusqu'à 1 000 livres) lorsque le téléphone était verrouillé et en mode de déplacement. Cette découverte a démontré le rôle vital que les analystes de sécurité et les chercheurs de menaces ont à jouer pour protéger les entreprises et les clients contre les risques de cybersécurité potentiels associés à la technologie de paiement. Les technologies de paiement impliquant la biométrie vont nécessiter des mesures de cybersécurité semblables à celles décrites dans la section Réalité mixte ci-dessus. De même, pour les détaillants qui font appel à des fournisseurs externes pour les services de paiement demandés par leurs clients, nous leur suggérons de consulter la section ci-dessus concernant la chaîne d'approvisionnement numérique afin de bénéficier de conseils sur la manière d'empêcher les dommages provoqués par des attaques visant des parties tierces de votre écosystème plus large.

Suggestions :

- Vérifiez que les appareils anciens de votre entreprise (y compris les points de vente) sont protégés à l'aide d'une technologie de sécurité appropriée aux systèmes embarqués : le logiciel de paiement que vous adoptez risque de ne pas être optimisé pour des appareils plus anciens dont vous dépendez.
- Menez des analyses de vulnérabilité régulières et soyez absolument certain que vous disposez naturellement d'une surveillance des menaces adaptée intégrée à la configuration de votre cybersécurité.
- Placez la confidentialité des consommateurs comme priorité pour la sécurité de vos paiements, toute fuite de leurs données financières personnelles étant potentiellement dévastatrice pour votre réputation.
- Tenez compte du conseil de l'industrie des cartes de paiement concernant la norme de sécurité sur les données (PCI DSS) : « La conformité PCI est un processus permanent », élaboré autour d'une boucle continue d'évaluation, de correction et de signalement.
- Assurez-vous que tous les appareils de paiement mobile peuvent être chiffrés à distance en cas de vol, de perte ou de compromission.

Tendance n° 5 : Analyse du commerce de détail – IA et algorithmes

L'analyse des données constitue un cas où la quantité et la qualité semblent avoir une égale importance. Sans transformer leur utilisation de l'analyse grâce à des technologies d'IA et algorithmiques, les détaillants vont s'efforcer de concrétiser la promesse de commerce unifié, ou d'optimisation de la chaîne d'approvisionnement et de la planification.

Le marché de l'analyse du commerce de détail devrait croître de 4,3 milliards de dollars en 2020 jusqu'à 11,1 milliards de dollars d'ici 2025. Cela représente un taux de croissance annuelle composé de 21,2 %.

Qu'y a-t-il de différent à l'heure actuelle en ce qui concerne l'analyse du commerce de détail ? La réponse est simple : le commerce de détail algorithmique. Selon les termes de Gartner, la « le commerce de détail algorithmique connecte le « Big Data » aux résultats, en faisant le chemin de l'analyse descriptive vers l'analyse descriptive. Ce basculement, de « descriptive » vers « prescriptible » est l'une des plus grosses modifications qui ait jamais touché le secteur.

Du seul point de vue culturel et organisationnel, la transition vers une analyse descriptive présente une rupture énorme, dans le sens favorable du terme. Pour les détaillants, l'un des défis va consister à attirer et à retenir des personnes qui sont en mesure de les guider dans leur utilisation du commerce de détail algorithmique. C'est un domaine hautement spécialisé, qui doit être traité correctement.

Avec le commerce de détail algorithmique, l'industrie a finalement accès à une technologie qui va alimenter des cas d'utilisation de l'IoT (notamment l'inventaire) et exploiter le potentiel de l'IA jusqu'à de nouveaux niveaux. Le commerce de détail algorithmique présente actuellement un taux de pénétration de 20à 50 %, et une évaluation des bénéfices « radicalement différente » selon Gartner : sans surprise, étant donné les possibilités d'optimisation et d'automatisation entre les secteurs qu'elle offre.

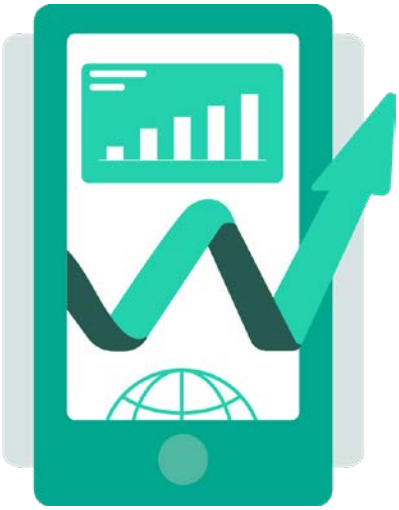
Comment utiliser la technologie d'analyse du commerce de détail en toute sécurité ?

L'utilisation réussie de l'analyse, en particulier de ses itérations d'IA et algorithmiques émergentes, nécessite de votre part de disposer d'un ensemble de données suffisamment grand (énorme) par rapport auquel le système peut tester les algorithmes qu'il génère. À l'évidence, l'agrégation de telles données, et leur mise à la disponibilité d'un système d'analyse algorithmique, présente un éventail de risques de sécurité et de confidentialité qui doit réellement être pris très sérieux.

Dans le même temps, toute crainte à propos de ces risques peut se transformer à son tour en risque : voir des concurrents plus courageux adopter l'analyse d'IA et assister à l'envolée de leurs profits par rapport à ceux d'entreprises plus prudentes.

Suggestions :

- Utilisez la fonctionnalité EDR extrêmement proactive pour rechercher des menaces avant qu'une quelconque violation ne puisse être tentée. La découverte des menaces n'est pas toujours suffisante, c'est la raison pour laquelle la recherche des menaces entre en scène.
- Élaborez une formation de sensibilisation à la cybersécurité selon les normes de vos politiques de ressources humaines afin de vous assurer que vos employés ont les moyens de devenir une partie intégrante de votre rempart contre les attaques. Même lorsque vous comptez sur l'IA pour l'analyse, il n'existe pas d'alternatives au travail effectué par des êtres humains correctement formés.
- Envisagez de sous-traiter une partie du fardeau de votre cybersécurité à un fournisseur de services gérés, afin de bénéficier d'une expertise de sécurité de haut niveau extrêmement spécialisée, tout en déchargeant votre personnel informatique pour qu'il puisse concentrer sur les tâches qui nécessitent absolument son attention.
- Assurez-vous que la configuration de votre sécurité et votre stratégie adoptent une approche unifiée vers les deux lieux de votre parc informatique : votre infrastructure d'exploitation centrale (par exemple, les terminaux) et les appareils (par exemple, les points de vente) et les capteurs (IoT) sur lesquels repose votre activité.



Tendance n° 6 : Marketing agile

La frontière entre les expériences de commerce de détail en ligne et hors ligne est désormais plus floue que jamais, ce qui génère des questions à la fois basiques et extrêmement complexes. Par exemple : où se trouvent vos clients ?

Le marketing de commerce de détail traditionnel, segmenté (à des degrés divers) par canal ou nœud de réalisation, sans recouvrement notable, n'est pas adapté au monde du commerce unifié ou omnicanal.

Vous savez déjà que vos clients sont ici, là et partout. Aujourd'hui, la différence réside dans la vitesse à laquelle ils se déplacent entre le monde en ligne et hors ligne. Et il ne s'agit pas simplement d'une question de vitesse : les clients s'attendent à ce que les demandes fonctionnent en parallèle et en synergie.

Le marketing agile ne consiste pas à voir le client comme une cible mouvante (votre défi étant de le « toucher » au passage entre les deux mondes).
Le marketing, vu auparavant comme une forme de fonction administrative, se trouve désormais aux côtés de fonctions que nous imaginons généralement lorsque nous abordons les cinq autres tendances dans ce document.

Le marketing agile correspond à l'extension de la technologie prometteuse de l'IA et du commerce de détail algorithmique (par exemple) pour prescrire des activités de marketing, et élaborer une automatisation dans le processus. L'exploitation de la technologie pour créer une réalisation omnicanal ou un commerce unifié ne fait aucun sens si la même technologie n'est pas en mesure de rassembler les données de la fonction marketing et d'informer les activités de celle-ci.

Comment utiliser le marketing agile en toute sécurité

Réglementation du marketing agile

Depuis le RGPD, la fonction marketing a été soumise à la pression des régulateurs pour protéger la vie privée des consommateurs. Ce n'est pas que la fonction marketing soit le seul aspect qui ait trait aux données privées des consommateurs ; toutefois, à la différence de la fonction financière, elle n'a pas été habituée à subir les pressions de la conformité réglementaire.
Les technologies telles que la réalité mixte vont amener de nouveaux niveaux de pression réglementaire à la fonction marketing. C'est une chose que de connaître le nom, l'adresse e-mail et le comportement social d'un client, mais c'en est une autre que d'avoir accès à son comportement via des technologies comme la réalité mixte. Cependant, les données obtenues par la réalité mixte (par exemple) sont une source dont les services marketing ne voudront pas être privés, tout particulièrement dans la mesure où l'évolution vers des approches agiles continue de s'accélérer.

Deux mots : Expérience globale. La chose merveilleuse en ce qui concerne le service marketing à partir de 2021 et au-delà est qu'il se trouve déjà dans une position parfaite pour fonctionner avec d'autres fonctions d'une manière réellement « commune ». Le concept d'expérience globale (une évolution du principe selon lequel les clients n'achètent pas des produits, mais des « expériences ») existe déjà depuis quelques années maintenant, mais les technologies telles que la réalité mixte et la croissance exceptionnelle du commerce électronique mobile en ont fait désormais une réalité. La bonne nouvelle est que les analystes, tels que Gartner, recommandent d'unifier l'expérience de gestion et l'expérience employé avec l'expérience client et l'expérience utilisateur. En bref, les services marketing avisés savent que pour offrir l'expérience globale désormais attendue par les clients, ils doivent travailler de concert avec d'autres services de l'entreprise, et cela inclut le service informatique. Cette collaboration fonctionne évidemment dans les deux sens, en présentant de nouvelles opportunités pour une compréhension et une coopération entre les services, éliminant avec un peu de chance les cloisonnements en matière de sécurité et de données, et en facilitant comme jamais l'implication de tout le monde envers la stratégie et les pratiques de sécurité de l'entreprise.

Suggestions :

- Élaborer une cyberculture extrêmement positive, dans laquelle tous les employés sont encouragés à être fiers du rôle qu'ils ont à jouer pour garantir la sécurité de leur activité, et celle des clients. Rendre les formations aux techniques de cybersécurité disponibles si besoin, et inclure la sécurité comme indicateur de performance clé pour les employés lorsque cela est pertinent dans les évaluations de performance annuelles.
- Ne jamais oublier que même si les outils du marketing agile basés sur l'IA tels que Black Swan peuvent représenter une promesse immense pour les distributeurs au détail, le rôle de l'instinct de l'être humain continuera à constituer un puits riche en inspiration pour le marketing, sans parler d'une source essentielle de « mécanismes régulateurs » pour la sécurité de n'importe quel outil marketing automatisé, quelle que soit son agilité.
- Gardez à l'esprit que plus vous employez l'IA pour vos activités marketing, plus ou vous aurez nécessairement un nombre important de donnés clients à exposer. Cela ne vaut pas la peine d'aller de l'avant sans mesures de cybersécurité appropriées pour protéger les données financières et d'autres données personnelles de vos clients. La règle est : la sécurité d'abord, toujours. Un gain marketing à court terme ne vaut pas la peine de sacrifier votre réputation sur le long terme.

Résumé

En 2020, le secteur du commerce de détail est parvenu à condenser environ 5 ans de transformation numérique en l'espace de quelques semaines, s'avérant être un réel leader en matière d'agilité parmi les autres secteurs. Comme nous arrivons à la fin de 2021, la tâche consiste à capitaliser sur cette impulsion héroïque, à consolider les gains, et à faire des progrès encore plus grands vers les immenses possibilités offertes par les technologies innovantes du commerce de détail. Comme toujours, les détaillants doivent avoir une confiance totale dans le fait que leur transformation numérique est sécurisée. La bonne nouvelle est que Kaspersky peut vous aider à évoluer et à vous adapter quoi qu'il arrive demain, en facilitant la protection de votre entreprise, et celle de vos clients, tout en vous transformant audacieusement et avec assurance au cours de la prochaine décennie et au-delà.

Aider les détaillants au niveau mondial signifie offrir des solutions qui leur sont adaptées. Bien que tous les détaillants soient des héros, aucune activité n'est semblable. Nous rencontrons nos clients détaillants là où ils se trouvent, en accordant en permanence la priorité à la continuité de l'activité et à l'innovation libérée de toute crainte.

Tout ce que nous faisons s'appuie sur la Threat Intelligence de Kaspersky reconnue mondialement, en renforçant notre recherche durable pour protéger les données, les clients et la continuité de l'activité 24h/24, 7j/7 contre les menaces avancées et les attaques ciblées.

Parcourez le portefeuille des produits Kaspersky pour les entreprises pour trouver les solutions et les services qui vous aideront à innover sans mettre votre activité (ou celle de vos clients) en danger. Pour vous aider à trouver le produit parfaitement adapté, nous avons organisé notre portefeuille par étapes. Parce que quel que soit le stade où vous en êtes dans votre parcours vers l'innovation, Kaspersky vous aidera à vous projeter dans le futur avec une conviction totale.

Approche de la cybersécurité par étapes de Kaspersky

1

Kaspersky Security Foundations – protection de base essentielle automatisée et basée sur le cloud pour tous les appareils, infrastructures VDI et serveurs hybrides, avant que les organisations progressent en douceur vers...

2

Kaspersky Optimum Security - pour les organisations nécessitant une sécurité plus spécialisée contre les menaces nouvelles et vagues, avant de mettre en œuvre de manière fluide notre troisième version...

3

Kaspersky Expert Security – pour les organisations disposant d'équipes de sécurité informatique établies et matures luttant contre les attaques ciblées les plus complexes.

Cybersécurité niveau de maturité	Solution
Informatique Petites entreprises ne disposant d'aucune équipe spécialisée dans la sécurité informatique	**Quoi** Kaspersky Security Foundations **Comment** Mise en œuvre des éléments fondamentaux de la sécurité pour les organisations de toutes tailles et complexité, en délivrant une prévention automatique gérée dans le cloud contre les cybermenaces liées aux produits courants sur tous les appareils, les infrastructures VDI et de serveur hybride. ▸ **Terminaux :** Protégez chaque terminal de votre organisation avec Kaspersky Endpoint Security for Business ; Kaspersky Embedded Systems Security ▸ **Cloud :** Bénéficiez d'une sécurité sans limite avec Kaspersky Hybrid Cloud Security ▸ **Réseau :** Sécurisez votre périmètre avec Kaspersky Security for Mail Server ; Kaspersky Security for Internet Gateway ▸ **Données :** Protégez les données précieuses et sensibles avec Kaspersky Security for Storage ▸ **Gestion de la sécurité :** Accédez à l'expertise avec Kaspersky Premium Support ; Services professionnels Kaspersky
Cybersécurité Entreprises à la recherche d'une défense avancée, mais disposant de peu de ressources spécialisées en sécurité informatique	**Quoi** Kaspersky Optimum Security **Comment** Lutte contre les menaces évasives, grâce à une détection et une intervention efficaces sur les terminaux, ainsi qu'à un suivi continu de la sécurité, le tout sans les coûts prohibitifs et la complexité associés ▸ **Détection avancée :** Optimisez l'analyse comportementale fondée sur l'apprentissage machine, le sandboxing, la Threat Intelligence et la recherche de menaces automatisée* avec Kaspersky Sandbox, Kaspersky Threat Intelligence Portal et Kaspersky Managed Detection and Response Optimum ▸ **Analyse et investigation :** améliorez la visibilité des menaces et le processus d'enquête simplifié avec Kaspersky Endpoint Detection and Response Optimum ▸ **Réponse rapide :** déployez des options de réponse automatisées dans le produit, ainsi que des scénarios de réponse guidée et gérée* avec Kaspersky Endpoint Detection and Response Optimumet Kaspersky Managed Detection and Response Optimum ▸ **Sensibilisation à la sécurité :** équipez les employés avec des outils automatisés à tous les niveaux et développez des compétences de cybersécurité essentielles avec la formation de sensibilisation à la sécurité de Kaspersky *Soutenu par les experts Kaspersky

Équipe de sécurité informatique expérimentée et parfaitement qualifiée et/ou SOC dédié

- Disposent d'un environnement informatique complexe et distribué
- Constituent une cible privilégiée pour les attaques complexes et de type APT
- Ont une aversion pour le risque en raison des coûts élevés des incidents de sécurité et des violations de données
- Sont concernées par la conformité aux réglementations

Quoi
Kaspersky Expert Security

Comment
Maîtrise totale des cyberattaques les plus complexes et les plus ciblées

- **Équipé :** Donnez à vos experts internes les moyens de faire face à des incidents complexes dans le domaine de la cybersécurité. Profitez d'une solution de cybersécurité unifiée. **La plate-forme Kaspersky Anti Targeted Attack Platform,** qui repose sur **Kaspersky EDR**, offre à votre équipe des capacités XDR.
- **Informé :** approfondissez vos connaissances avec la Threat Intelligence et développez les compétences de vos experts pour gérer les incidents complexes :
  - Intégrez des informations sur les menaces immédiatement exploitables dans votre programme de sécurité. **Kaspersky Threat Intelligence** vous donne un accès instantané à une solution de Threat Intelligence technique, tactique, opérationnelle et stratégique.
  - Grâce à la **Kaspersky Cybersecurity Training**, développez les compétences pratiques de votre équipe interne, notamment en ce qui concerne l'utilisation de preuves numériques, l'analyse et la détection de logiciels malveillants, ainsi que l'adoption de pratiques exemplaires dans le cadre de la réponse aux incidents.
- **Renforcé :** faites appel à des experts externes pour assurer une évaluation de la sécurité, une assistance immédiate et un soutien :
  - Profitez de l'assistance immédiate de l'équipe **Kaspersky Incident Response**, composée d'analystes et d'enquêteurs très expérimentés, pour résoudre votre cyberincident de manière rapide et efficace.
  - Avec Kaspersky **Managed Detection and Response**, vous bénéficiez d'un deuxième avis et de l'expertise d'un partenaire de confiance en matière de Threat Hunting. Vos experts internes en sécurité informatique disposent ainsi de plus de temps pour réagir aux problèmes critiques qui requièrent leur attention.
  - Déterminez le niveau d'efficacité de vos défenses contre les cybermenaces potentielles et si vous représentez déjà la cible involontaire d'une attaque furtive à long terme, grâce à **Kaspersky Security Assessment**.

Solutions ciblées

Quoi	Comment
 **Kaspersky Embedded Systems Security**	Une solution à plusieurs niveaux offrant une protection inégalée aux appareils embarqués basés sur Windows, même pour ceux disposant de ressources système limitées et exécutant des systèmes d'exploitation obsolètes. Des niveaux de sécurité incluant le contrôles des applications et des appareils, un mécanisme de prévention des vulnérabilités et des solutions contre les programmes malveillants, ce qui signifie que la protection peut être optimisée pour les appareils disposant de peu de ressources, notamment les anciens PC exécutant des systèmes d'exploitation qui ne sont plus pris en charge, tels que Windows XP.
 **Kaspersky Fraud Prevention**	Advanced Authentication (l'authentification avancée) permet une authentification sans friction et continue, réduisant les coûts de traitement du deuxième facteur de l'authentification pour les utilisateurs légitimes, tout en conservant des taux de détection de fraude élevés en temps réel. Automated Fraud Analytics analyse minutieusement les événements qui se produisent au cours de l'intégralité de la session en les transformant en données précieuses. Protège le périmètre extérieur de n'importe quelle entreprise, assurant la sécurité et la protection des clients.
 **Kaspersky DDoS Protection**	Couvre une bande passante allant jusqu'à 2 Gbits/s, avec couverture de service étendue, comprenant les rapports d'analyse d'attaque et les évaluations de capacité anti-DDoS. Atténuation des risques DDoS permanente et automatique facultative, enrichie par les ingénieurs de Kaspersky qui effectuent des vérifications parallèles pour optimiser la défense en fonction de la nature de chaque attaque DDoS.
 **Kaspersky Payment Systems Security Assessment**	Met en évidence la moindre vulnérabilité dans votre infrastructure de points de vente susceptible d'être exploitée pour différents types d'attaques, pointe les conséquences possibles, évalue l'efficacité de vos mesures de sécurité actuelles et vous aide à établir un plan d'action pour corriger les failles et renforcer votre protection.

Actualités sur les cybermenaces : www.securelist.com

Actualités dédiées à la sécurité informatique : www.kaspersky.com/blog

Portail de Threat Intelligence : opentip.kaspersky.com

Aperçu des technologies : www.kaspersky.com/TechnoWiki

Prix et distinctions : https://www.kaspersky.fr/about/awards

Portefeuille produits interactif : kaspersky.com/int_portfolio

kaspersky PRÊTS POUR L'AVENIR