Analyse sur l'authentification intelligente et la prévention des fraudes

Solutions pour faire face aux nouveaux défis dans le domaine de l'expérience client (CX) et des risques de sécurité »

opusresearch

opusresearch | Rapport »

Analyse sur l'authentification intelligente et la prévention des fraudes

Solutions pour faire face aux nouveaux défis dans le domaine de l'expérience client (CX) et des risques de sécurité »

Dans ce troisième rapport annuel, Opus Research et SymNex Consulting fournissent aux décideurs du monde de l'entreprise le contexte concurrentiel nécessaire pour évaluer une sélection de fournisseurs de solutions pour la prévention des fraudes et des interactions clients sécurisées. L'authentification intelligente (IAuth) regroupe une gamme de produits et de services qui vont au-delà de la biométrie vocale pour inclure d'autres facteurs biométriques (biométrie faciale, digitale, comportementale), la détection des fraudes, l'orchestration numérique et l'authentification en continu. Ce rapport évalue 20 marques (fournisseurs de plateformes et fournisseurs de technologies clés) afin de comprendre la richesse de leurs offres et leur capacité à orchestrer les fonctionnalités pour créer des solutions complètes qui répondent aux nouveaux défis dans le domaine de l'expérience client et des risques de sécurité.

»

Août 2020

Dan Miller, analyste principal et fondateur d'Opus Research
Matt Smallman, directeur de SymNex Consulting
Derek Top, directeur de recherche chez Opus Research

SYMNEX

Opus Research, Inc.
893 Hague Ave.
Saint Paul, MN 55104

www.opusresearch.net

» Sommaire

SOMMAIRE DES ILLUSTRATIONS

L'authentification est la première impression donnée par l'entreprise

Dans les années 1960, une marque de vêtements pour homme avait pour slogan publicitaire « pour la première impression, on n'a qu'une seule chance ». Ce slogan a aujourd'hui une nouvelle signification et une nouvelle pertinence face au nombre croissant de discussions commerciales qui se prolongent dans le temps, sur différents appareils. Après avoir cherché sur Internet, consulté des « amis » sur les réseaux sociaux et navigué sur différents sites de vente en ligne, la dernière chose que souhaite un prospect potentiel ou un client c'est d'avoir à se creuser la tête pour retrouver son mot de passe ou répondre à des questions de sécurité.

Pendant des décennies, les imposteurs ont considéré les centres de contact comme le talon d'Achille de l'entreprise dans la lutte pour empêcher les piratages et leurs conséquences (perte de données clients ou vol à grande échelle de biens, de services et de fonds). Depuis longtemps, les procédures d'authentification ont remplacé le « que puis-je faire pour vous ? » comme première étape (ou barrière) du service ou de l'assistance client. Ces procédures se sont révélées longues, frustrantes et inefficaces. Les pratiques les plus courantes sont notamment l'envoi par SMS de « mots de passe à usage unique » et l'authentification basée sur des connaissances. La première méthode est vulnérable aux attaques dites « de l'homme du milieu » (man-in-the-middle attack) rudimentaires et la seconde repose essentiellement sur des informations que les imposteurs peuvent compiler à partir de sources publiques.

Opus Research définit l'« authentification intelligente » comme une gamme de produits et de services qui vont au-delà de la biométrie vocale pour inclure des facteurs biométriques supplémentaires (biométrie faciale, digitale, comportementale), la détection des fraudes, l'orchestration numérique et l'authentification en continu.

Accélération sur la voie de la maturité

Depuis leur apparition, les initiatives en matière d'authentification client se sont bornées à utiliser une courte liste de facteurs pour neutraliser les fraudeurs tout en permettant aux clients identifiés de mener à bien leurs démarches. Les codes PIN et mots de passe (quelque chose que vous êtes seul à connaître) ont été privilégiés, associés à des questions de sécurité ou à d'autres formes d'authentification basée sur des connaissances. Trop souvent, elles exigeaient des clients de faire eux-mêmes le travail pénible : mémoriser un mot de passe, répondre à une série de questions de sécurité ou demander, puis saisir un « mot de passe à usage unique » affiché sur un téléphone portable ou le « dongle » de l'entreprise.

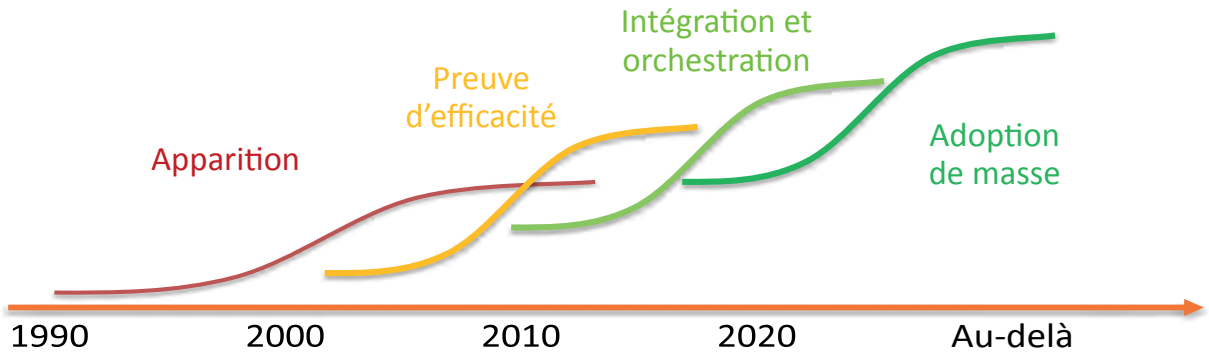
Les solutions modernes doivent faire beaucoup plus. Rappelez-vous qu'aucun client n'appelle ou ne va sur un site Web pour s'authentifier ; ils ont en tête un objectif ou une intention précise et l'authentification est un mal nécessaire. Le dispositif doit avoir accès au contexte, c'est-à-dire à la localisation géographique du client, à l'historique de ses activités, de ses transactions et prendre en compte l'intention du moment pour en déduire le niveau de risque associé à un client ou une activité donnés. La procédure ne doit requérir aucun effort (ou alors minime) de la part du client afin de créer un lien de communication de confiance avec la marque. Les entreprises qui utilisent une procédure d'enregistrement passif pendant la discussion avec un SVI basé sur la reconnaissance vocale, un assistant virtuel ou en direct avec un agent arrivent en tête dans notre évaluation.

Stades d'évolution de l'authentification intelligente

Les solutions d'authentification intelligente (plateformes et technologies clés) ont évolué en même temps que (et pour appuyer) la transformation numérique, les assistants intelligents et l'IA conversationnelle. Le phénomène a lentement commencé au tournant du siècle, suscitant des inquiétudes quant à la

précision et à la rentabilité. [Voir la figure 1 ci-dessous représentant l'évolution de l'authentification intelligente.] Une fois l'adhésion des premiers utilisateurs (à savoir des adolescents) clairement démontrée, l'adoption et la mise en œuvre se sont considérablement accélérées et se sont poursuivies dès que le retour sur investissement a été prouvé.

Figure 1 : les différents stades d'évolution de l'authentification intelligente



Facteurs	Un seul facteur (voix, par ex.)	2 facteurs	Multifacteurs	Continuité
Obstacles à l'adoption	Précision	Adhésion des utilisateurs	ROI	Aucun
Contexte	SVI automatisé	Centres de contact	Applications en langage naturel	Migration vers le cloud
Produits et services	Auth vocale dépendante du texte	Auth et enregistrement actifs et passifs	Détection des fraudes et auth à plusieurs niveaux, tenant compte des risques	Auth continue, sans effort et détection des fraudes passives

- **Apparition** (2000-2010) : l'approche « ma voix est mon mot de passe » se fonde sur l'utilisation consciente par l'appelant de sa voix (ce qu'il est) en lieu et place d'un code PIN ou mot de passe (ce qu'il est seul à connaître). Les solutions étaient rigides (dépendantes du texte) et suscitaient la suspicion, en particulier chez les professionnels de la sécurité dont l'objectif était « zéro faux positif ».
- **Preuve d'efficacité** (2011-2017) : les fournisseurs de solutions ont enregistré un milliard d'empreintes vocales dans les systèmes de banques, d'entreprises de télécommunications, de prestataires de services de santé et d'administrations publiques pour accélérer l'authentification et dissuader l'accès frauduleux. La détection des fraudeurs en temps réel à l'aide de différentes technologies, notamment les réseaux de neurones multicouches combinés à la biométrie vocale passive, ont joué un rôle essentiel pour justifier l'investissement.
- **Intégration/Orchestration** (2018-2020) : les professionnels de l'UX, de la sécurité et des architectures informatiques joignent leurs efforts à ceux des équipes opérationnelles du centre de contact pour intégrer différents procédés biométriques, moteurs de risque, outils de conception d'UX et autres plateformes de gestion de workflow pour créer des solutions adaptées au monde réel. Tous reconnaissent la valeur de l'authentification forte en temps réel pour améliorer la sécurité, l'expérience client et les initiatives de personnalisation.
- **Adoption de masse** (ambitieuse) : la solution proposée par les entreprises évaluées dans ce document a séduit par sa capacité à répondre au besoin de procédures simples d'authentification forte, avec des stratégies de mise sur le marché qui la rendent abordable pour toutes les entreprises ayant une relation durable avec leurs clients. Après la pandémie du Covid, cela signifie des opportunités non plus seulement pour les banques, les prestataires de services financiers et les entreprises de télécommunications mais aussi pour le commerce en ligne, la télémédecine et les services publics en ligne.

Point de vue client

« Le projet a démarré en avril 2016 avec l'objectif de renforcer la sécurité, réduire le délai de traitement et limiter les questions de sécurité pénibles nécessaires à l'authentification... Les difficultés étaient principalement d'ordre juridique, en raison de la loi sur la protection des données et du choix nécessaire entre opt-in et opt-out [...] Après quelques ajustements, l'étude de rentabilité a pu être finalisée. »

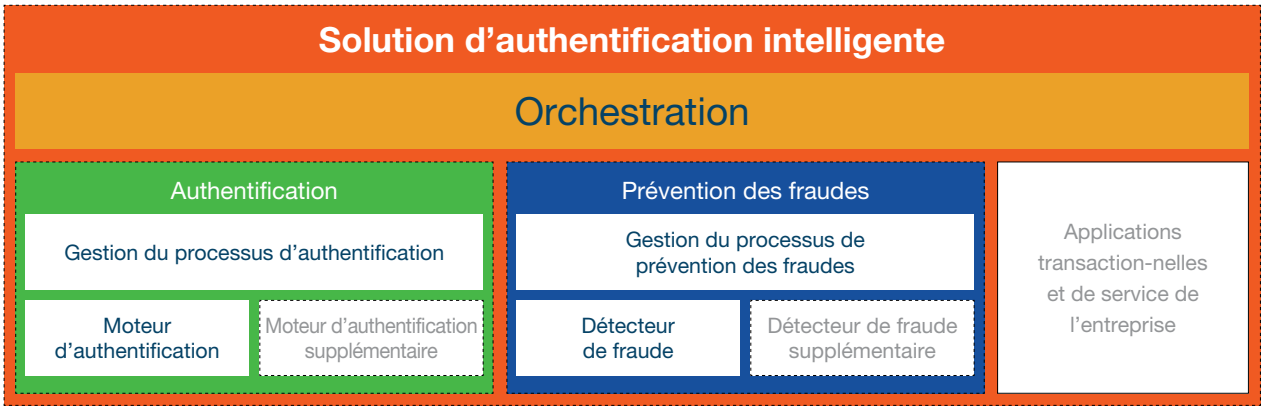
— Banque mondiale regroupant 2,5 M de clients particuliers, 300 000 clients professionnels, 500 agents de centre d'appels

Authentification intelligente et détection des fraudes à la loupe

Une solution d'IAuth complète intègre les fonctionnalités d'authentification et de détection des fraudes à la technologie sous-jacente du canal de communication, aux processus métiers requis pour authentifier le client (enregistrement et vérification) ou à la détection des fraudes (liste noire, gestion des cas) et entre elles pour créer un service client sécurisé. Dans un grand nombre d'entreprises, cette « pile » consiste à combiner des solutions personnalisées ou packagées de différents fournisseurs avec des fonctionnalités développées en interne. Sur la figure 2 (ci-dessous), nous disséquons les couches et les composants conceptuels de cette pile afin d'aider le lecteur à articuler plus clairement ses besoins.

Au fil de la maturation du marché de l'authentification intelligente ces dernières années, nous avons vu se développer des domaines d'attention distincts chez les prestataires et pour les entreprises. Certains prestataires font le choix de se spécialiser dans une ou deux « technologies clés » pour répondre aux besoins ou aux exigences des développeurs d'applications avec des solutions intégrées. Une autre catégorie de prestataires a une approche holistique plus conforme à notre définition de l'IAuth et plus apte à satisfaire ou à orchestrer une gamme complète de fonctions d'authentification et de détection des fraudes.

Figure 2 : dissection de la pile d'authentification intelligente



SOURCE : Opus Research (2020)

Pile d'authentification

La pile d'authentification, représentée ci-dessus en vert, comporte deux composantes clés pour l'entreprise et ses agents.

- Gestion du processus d'authentification – Cette couche fournit les fonctionnalités métiers pour le contact avec la clientèle, qui permettent d'utiliser un ou plusieurs moteurs principaux dans le processus d'authentification, par exemple pour gérer le consentement, l'enregistrement et la vérification du client. La majorité des composants d'authentification exposent uniquement une API qui peut être utilisée par l'organisation ou l'intégrateur système pour développer ledit composant.

- Moteur biométrique ou autre moteur d'authentification – Le composant d'authentification effectue la correspondance entre les nouvelles entrées et les modèles stockés. Dans le contexte du service client, il s'agit souvent d'un facteur biométrique comportemental ou physique mais des processus d'authentification basés sur des connaissances peuvent aussi être intégrés. En plus d'établir des correspondances, la solution doit se protéger des vulnérabilités connues (détecter les attaques de présentation et d'usurpation, par exemple).

Pile de prévention des fraudes

La pile de prévention des fraudes comporte elle aussi deux couches :

- Gestion du processus de prévention des fraudes – Cette couche est celle où les alarmes d'un ou plusieurs détecteurs permettent d'évaluer le risque de fraude de l'interaction et de déclencher les actions métiers requises, soit sous forme de gestion de cas soit en communiquant avec d'autres applications.

- Détecteur de fraude – Ce composant interprète le signal transmis par le canal sous forme de résultats pertinents, par exemple détection d'anomalies dans l'audio, signalement de caractéristiques ou établissement de correspondances avec les signatures de fraudeurs connus.

Orchestration

Le terme d'orchestration fait le plus souvent référence à l'utilisation de processus automatiques, d'algorithmes ou de règles pour configurer, gérer et coordonner des systèmes informatiques, des applications et des services. Plus spécifiquement, il peut désigner des ressources utilisées pour automatiser un processus ou un workflow comportant de nombreuses étapes dans une multiplicité de systèmes. Dans le contexte de l'IAuth, l'orchestration coordonne les processus d'authentification et de prévention des fraudes en utilisant du contexte supplémentaire fourni par d'autres applications transactionnelles ou de service de l'entreprise pour déterminer si l'interaction ou la transaction peut se poursuivre avec ou sans étapes additionnelles d'authentification ou de prévention des fraudes. Le dispositif repose généralement sur un « score de risque » qui détermine comment l'entreprise doit traiter l'individu ou la tâche spécifique qu'il ou elle effectue.

Les fonctionnalités d'orchestration sont souvent un facteur de différenciation entre les fournisseurs de plateformes complètes d'IAuth. Un groupe relativement restreint de prestataires propose des offres qui vont au-delà de l'authentification, la prévention des fraudes et l'orchestration. Par le biais de connecteurs ou d'API, ces solutions intègrent des informations issues de bases de données associées à d'autres applications ou services, qui permettent d'évaluer les risques et d'identifier les actions à mettre en œuvre sur la base de cette évaluation.

Point de vue client

« La principale difficulté est de produire un système évolutif et sécurisé qui peut être déployé et utilisé facilement par les entreprises et les particuliers. […] [La solution] remplace l'authentification par une vérification biométrique vocale et faciale gérée par le système avant la mise en relation avec un agent pour lui faire gagner du temps et considérablement renforcer la sécurité. »

—Directeur commercial chez un spécialiste de la sécurité des informations basé au Royaume-Uni

Deux catégories d'entreprises évaluées

« Est-ce que je veux une plateforme fournie par un seul prestataire ou ce qu'il y a de mieux en termes de technologies ? ». Tous les centres de contact, spécialistes de l'expérience client et de la sécurité, chefs de projets et professionnels des achats se posent la question, quels que soient la taille de l'entreprise ou le secteur d'activité.

Point de vue client

[Pour sélectionner un fournisseur, nous voulions] une solution de biométrie vocale faisant partie de la même suite d'applications que le système d'enregistrement vocal et que l'outil de gestion des agents... La facilité d'accéder pour nos utilisateurs à un seul système [était un critère important].

—Prestataire de services financiers et bancaires basé en Asie-Pacifique

Pour préparer ce document, Opus Research a évalué les produits et services d'IAuth de 20 prestataires – 7 « fournisseurs de plateformes » et 13 fournisseurs de « technologies clés » – assurant l'authentification intelligente (IAuth) et la détection des fraudes. Ces dernières font partie des domaines d'opportunité représentés sur la figure 2 :

- **Fournisseurs de plateformes** : offrent des solutions clés en main qui prennent en charge l'enregistrement des empreintes vocales ou d'autres facteurs biométriques, l'authentification active ou passive et la détection des fraudes. Ils complètent leurs offres avec des technologies d'analyse, d'apprentissage automatique et des réseaux de neurones multicouches qui alimentent les moteurs de risque et les ressources de détection des fraudes. L'« orchestration » est un facteur de différenciation crucial. Elle utilise des moteurs décisionnels pour alimenter en information d'autres éléments de la plateforme d'après l'évaluation des données saisies en temps réel, par exemple le risque qu'un individu donné soit bien celui ou celle qu'il prétend, à l'emplacement géographique où il/elle est sensé(e) être, avec l'appareil qui lui est associé et qu'aucune autre anomalie n'est détectée.

- **Fournisseurs de technologies clés** : ette catégorie décrit des entreprises qui ont embauché du personnel et investi en continu dans des technologies destinées à créer un processus d'authentification forte, continue et sans friction dans le contexte du commerce conversationnel.

Figure 3 : entreprises prises en compte dans l'évaluation

Ce document (Annexe A) fournit un rapide profil des offres d'IAuth de chaque société et les positionne dans le « paysage de l'IAuth » d'après la qualité de leur offre de produits et leur position sur le marché.

Entreprise	Catégorie	Caractéristique
Aculab	Tech clé	Auth et sécurité basées sur des API
Auraya Systems	Tech clé	Spécialiste de la biométrie vocale
Biocatch	Société montante, à suivre	Biométrie comportementale, modèles d'IA
Daon	Plateforme	Sa plateforme IdentityX orchestre l'auth multifacteurs
ID R&D	Tech clé	Biométrie vocale de pointe + reconnaissance faciale, détection des voix enregistrées/synthétiques
Interactions	Société montante, à suivre	Authentification vocale intégrée à une plateforme d'agent virtuel intelligent
Journey	Société montante, à suivre	Orchestration d'auth « zéro connaissances », auth mutuelle
LumenVox	Tech clé	ASR, TTS, biométrie vocale et analyse conversationnelle
NICE	Plateforme	Authentification et prévention des fraudes en temps réel, détection en continu des fraudeurs grâce à l'IA
Nuance	Plateforme	Base de données d'empreintes vocales la plus importante au monde ; IA appliquée à la fraude et à l'orchestration
Nuestar-Trustid	Tech clé	Centre d'appels + numérique
Omilia	Plateforme	Self-service conversationnel
Phonexia	Tech clé	Biométrie vocale, analyse conversationnelle
Pindrop	Plateforme	Auth basée sur les risques ; détection des fraudes; intégration des réseaux de neurones multicouches
Sestek	Tech clé	Tech vocale étendue ; accent sur l'auth active
Spitch	Tech clé	Biométrie vocale essentielle, agent virtuel
Verbio	Tech clé	Biométrie vocale et traitement du langage
Verint	Plateforme	Biométrie vocale et comportementale pour l'authentification et la fraude
VBG	Tech clé	Spécialiste de la biométrie vocale, modèle SaaS ; API
VoiceIT	Tech clé	Biométrie vocale simple à déployer et différenciation en termes d'API

Critères d'évaluation pour l'IAuth

Pour garantir des conversations axées sur un objectif précis entre les marques et leurs clients, les entreprises doivent débuter différemment les interactions ou les échanges avec les appelants et les visiteurs de leurs sites Web. Pour ce faire, elles peuvent aujourd'hui appliquer l'analyse prédictive, les réseaux de neurones multicouches et l'authentification biométrique (digitale, vocale, faciale, comportementale) pour déterminer leur identité avant de poursuivre le dialogue. L'objectif visé en combinant ces technologies est l'authentification intelligente et la prévention des fraudes.

Dans ce document, Opus Research et SymNex Consulting évaluent les entreprises sélectionnées sur les critères suivants :

- En temps réel
- Qui tient compte des risques
- Adaptative
- Multifacteurs – biométrie comportementale y compris
- Multicouches

Toutes les sociétés étudiées se distinguent par la qualité de leurs offres de services. Pour aider le lecteur dans sa sélection d'un prestataire, elles ne doivent toutefois pas être soumises aux mêmes critères d'évaluation.

En d'autres termes, les fournisseurs de plateformes sont évalués sur l'exhaustivité de leurs offres et leur capacité à orchestrer la performance des différentes fonctionnalités qui participent à une authentification sans friction. Les fournisseurs de technologies clés sont quant à eux évalués sur leur investissement dans des technologies uniques et sur leur utilisation de connecteurs, d'API et d'une approche de commercialisation flexible, qui facilite l'intégration à des solutions plus larges, adaptées aux nouveaux défis en matière d'expérience client et de sécurité.

Dans le viseur : nouvelles solutions orientées IAuth

Membres qui n'appartiennent pas à une catégorie mais qui pourraient la transformer

Nous attirons particulièrement l'attention sur trois marques, comprises dans cette évaluation, bien que leurs offres de produits et services ne relèvent pas directement des catégories « plateforme » et « technologie clé ». Opus Research les considère comme des baromètres ou des fournisseurs d'avant-garde de technologies qui contribuent à faire avancer le concept d'IAuth, même si rien ne permet de les comparer directement à d'autres sociétés des deux catégories étudiées. Elles ont conçu de formidables gammes de services qui combinent les principes de l'IAuth et un sous-ensemble de composants de la solution complète.

Journey.ai
La solution Trusted Identity Platform de Journey.ai vise à combler des lacunes spécifiques dans l'infrastructure numérique du commerce conversationnel, en assurant un juste équilibre entre sécurité, confidentialité et expérience client sur les différents canaux. Son approche « zero trust » permet aux entreprises d'utiliser leurs applications mobiles et smartphones pour l'enregistrement des clients et agents, puis exploite les ressources pour faire appel de manière flexible à différents facteurs d'authentification, notamment la biométrie. Elle applique des techniques originales pour ce qu'elle nomme « l'authentification mutuelle » et intègre la biométrie comportementale à l'éventail des facteurs d'authentification pour assurer une expérience continue, fluide et sans friction.

BioCatch
Biocatch a mis au point une technologie clé de biométrie comportementale qui établit des profils à partir d'actions comme les déplacements de la souris, la cadence de frappe, la manière de balayer l'écran ou l'orientation de l'appareil. Ces profils, comparés à ceux de la population, permettent de détecter les fraudeurs ou les imposteurs. Pour les banques, les assureurs et les émetteurs de cartes de crédit, c'est un outil essentiel pour prévenir la fraude sur les « nouveaux comptes » et détecter les imposteurs, les robots et les voix « synthétiques » d'usurpateurs tentant d'accéder à des comptes existants.

Interactions LLC
La société Interactions est incluse dans cette évaluation car elle offre des fonctionnalités éprouvées d'authentification et de détection des fraudes basées sur la biométrie vocale en tant que complément naturel de son assistant virtuel vocal. Elle n'est pas commercialisée comme une technologie clé autonome ni intégrée à une plateforme d'IAuth plus large (s'appuyant sur des moteurs décisionnels et de risque). Opus Research pense que les ressources d'enregistrement et d'authentification d'Interactions constituent une alternative digne d'intérêt pour les entreprises qui utilisent ses assistants virtuels intelligents.

Schémas comparatifs des fournisseurs de plateformes et de technologies clés

Pour assister les décideurs dans leur évaluation des différents fournisseurs, Opus Research représente leur positionnement sur une série de schémas comparatifs. Sur les figures 4, 5 et 6 ci-après, nous avons représenté les fournisseurs de solutions d'après leur position et leur réussite respectives sur le marché. La taille des ellipses reflète deux facteurs cruciaux :

- **Exhaustivité/flexibilité du produit :** Pour que les fournisseurs de plateformes obtiennent le meilleur score en termes d'« exhaustivité », les services et fonctionnalités doivent couvrir toutes les colonnes de la pile de solutions : authentification, prévention des fraudes, orchestration et applications. Les fournisseurs de technologies clés sont jugés sur la capacité de leurs relations à s'intégrer aux fournisseurs de solutions complètes par le biais de connecteurs et d'interfaces de programmation d'applications (API).

- **Potentiel stratégique :** Pour les deux catégories de fournisseurs, cet indicateur reflète la manière dont la vision et la feuille de route répondent aux besoins technologiques actuels et à leur évolution dans le centre de contacts et au-delà. La capacité à prendre en charge des facteurs multiples, par exemple biométrie comportementale, et à intégrer de nouvelles technologies comme les réseaux de neurones multicouches sont un plus. De même que la capacité à gérer des applications dans les domaines de l'IdO, des terminaux intelligents et des appareils mobiles. L'écosystème de partenaires, d'intégrateurs et de développeurs de chaque entreprise est également pris en compte.

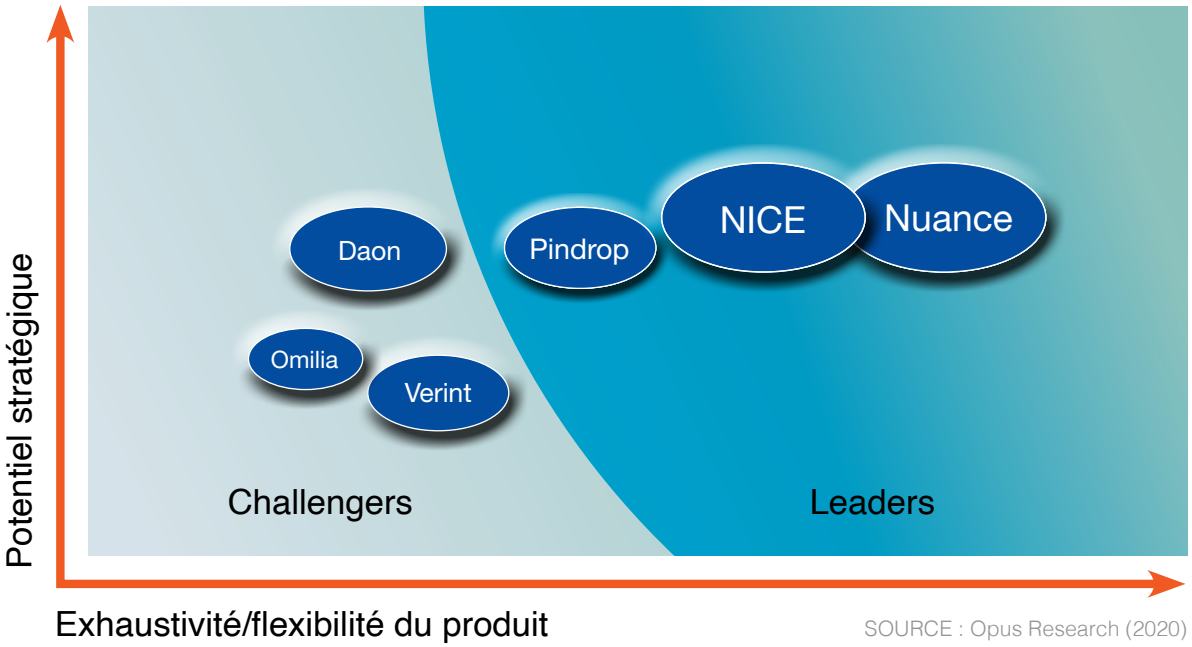
La taille des ellipses reflète la présence de chaque fournisseur, calculée d'après les informations fournies par l'entreprise ou des données publiques sur sa santé financière actuelle (chiffre d'affaires, rentabilité, solvabilité, longévité et taille de la clientèle).

La couleur des ellipses correspond à la catégorie de fournisseur :

Fournisseurs de plateformes

Fournisseurs de technologies clés

Figure 4 : schéma comparatif des fournisseurs de plateformes en 2020

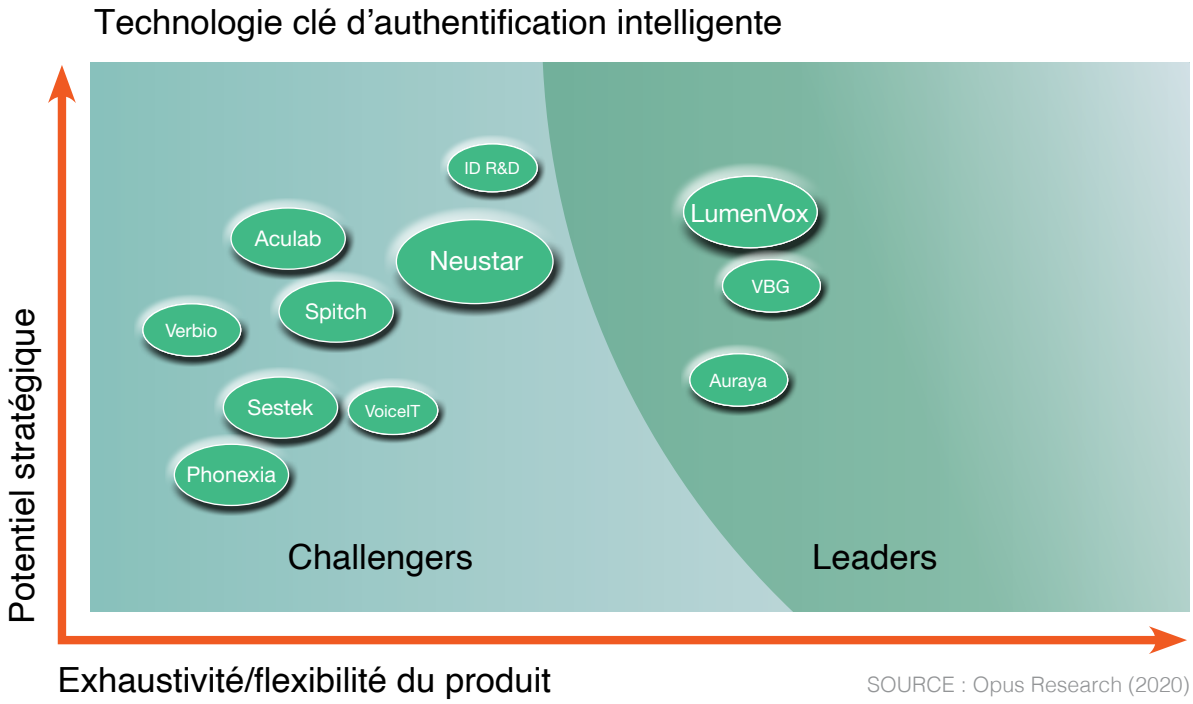


SOURCE : Opus Research (2020)

- Parmi les leaders de la catégorie des fournisseurs de plateformes, Nuance et NICE se distinguent par leurs technologies polyvalentes d'authentification, leurs offres intégrées pour la prévention des fraudes et une clientèle solide et bien établie. Les solutions regroupent : pour Nuance, Lightning Engine, ConversationPrint et DevicePrint ; pour NICE, la solution en temps réel ENLIGHTEN Fraud Prevention, qui utilise une technologie d'analyse conversationnelle basée sur l'IA et des modèles comportementaux pour fournir un feedback en temps réel aux agents.
- Pindrop s'est illustrée par sa technologie brevetée de vérification d'identité, des risques et de la fraude qui s'appuie sur une authentification basée sur les risques et sur une importante base de données de fraudeurs.
- Daon a réalisé des déploiements en production dans plusieurs pays du monde et ainsi permis d'authentifier des millions de transactions au moyen de multiples authentifications biométriques.
- Verint jouit d'une longue expertise dans le domaine de l'engagement client et de l'analyse conversationnelle et a constitué une liste de clients pour l'authentification et la prévention des fraudes.

- Grâce à l'intégration étroite entre son moteur d'authentification et sa plateforme d'IA conversationnelle, Omilia offre une solution attractive aux entreprises qui souhaitent utiliser ces deux technologies. Son moteur d'authentification est également disponible sous forme de composant autonome.

Figure 5 : schéma comparatif des fournisseurs de technologies clés en 2020

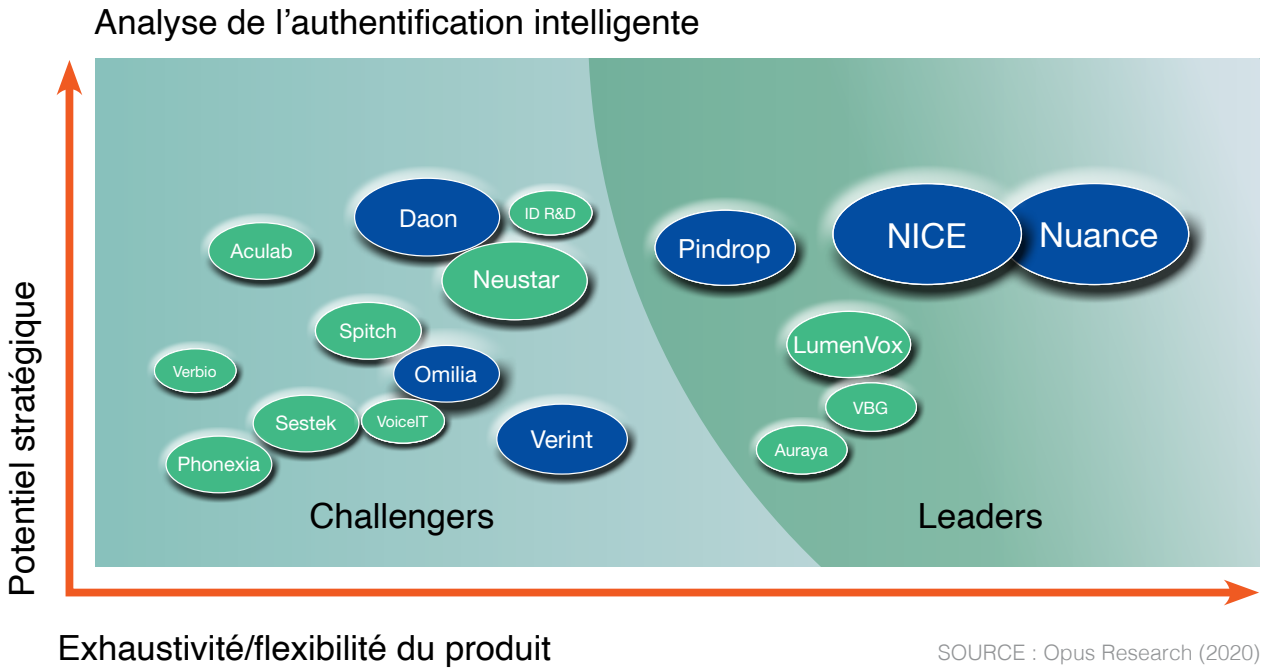


SOURCE : Opus Research (2020)

- La fusion entre LumenVox et VoiceTrust permet d'associer un fournisseur de solutions biométriques éprouvées à l'expérience d'intégration, de reconnaissance vocale et aux partenariats de LumenVox. Voice Biometrics Group (VBG) et Auraya sont axés sur la biométrie vocale et, avec plusieurs millions d'utilisateurs enregistrés, leurs solutions bénéficient d'une remarquable maturité et d'une grande expertise.
- ID R&D s'est spécialisée dans les créneaux applications et mobiles et a obtenu des résultats impressionnants aux tests. Neustar, avec l'acquisition de TRUSTID, combine des produits cross-canal destinés à l'authentification et à la prévention des fraudes dans le centre d'appels et sur les canaux digitaux.
- La proposition de service unique de VoiceIt ne nécessite qu'une simple carte de crédit pour démarrer et fournit suffisamment de code source pour les principales plateformes pour développer et déployer des applications en quelques heures au lieu de plusieurs mois.
- Verbio et Spitch ont développé des fonctionnalités de biométrie vocale en complément de leur gamme plus large de technologies vocales, comptent plusieurs déploiements à leur actif et se posent en véritables challengers sur leurs marchés. Avec plus de 40 ans d'expérience dans les technologies de traitement du signal et de la téléphonie, Aculab peut concurrencer les acteurs établis sur le marché de la biométrie vocale.

- Basée en Turquie, l'entreprise Sestek fournit une authentification vocale avec un large choix de solutions conversationnelles. Phonexia apporte au marché commercial son expérience de leader du marché des organismes d'État.

Figure 6 : schéma comparatif combiné des fournisseurs de solutions d'IAuth en 2020



SOURCE : Opus Research (2020)

Nuance

Siège social : Burlington, MA, É-U
Date de création : 1992
Chiffre d'affaires : ~1,5 milliard $
Nombre d'employés : ~8 500

Gamme de services d'IAuth :

Enregistrement et création de compte : prend en charge l'enregistrement sur les différents canaux. Dans chaque déploiement, l'appelant est soumis à une procédure d'enregistrement d'empreinte vocale soit de manière passive en parlant à un agent (dans le cas d'un centre d'appels) soit de manière active par le biais d'une phrase secrète. Pour les canaux digitaux, l'enregistrement peut être déclenché via une API pour la biométrie vocale, la biométrie comportementale et la biométrie faciale.

Authentification : Nuance fournit un large éventail de méthodes d'authentification, notamment biométrie vocale active (dépendante du texte), biométrie vocale passive (indépendante du texte), validation d'appel, ConversationPrint (choix du vocabulaire, grammaire et structure des phrases), DevicePrint (utilisation d'une empreinte unique pour identifier l'appareil d'après l'acoustique et le canal), reconnaissance faciale et biométrie comportementale. Nuance Lightning Engine permet une authentification indépendante du texte dans le SVI, avec une précision remarquable à partir d'énoncés très courts. Des détecteurs intelligents génèrent des signaux de familiarité ou de risque pour permettre une authentification en toute confiance. Nuance permet aussi d'ajouter des modalités biométriques et non biométriques supplémentaires par le biais de plugins, et un moteur de risque intégré pour gérer les processus d'authentification et de détection des fraudes d'après plusieurs facteurs.

Prévention des fraudes : Nuance permet de détecter la fraude sur les canaux vocaux et digitaux, et fournit une vue consolidée des activités à risque sur tous les canaux. Nuance peut détecter et analyser toutes les caractéristiques de fraude actuellement connues sur un canal (vocal et numérique), notamment identifier les caractéristiques vocales de l'imposteur (biométrie vocale) qui permettent de détecter le fraudeur, de l'identifier et de le poursuivre en justice en s'appuyant sur des preuves biométriques.

Nuance peut détecter un fraudeur d'après ses caractéristiques comportementales de langage, en particulier le choix du vocabulaire, la grammaire et la structure des phrases (ConversationPrint). Nuance fournit la seule solution de prévention des fraudes capable d'identifier un fraudeur d'après deux facteurs biométriques indépendants sur le canal vocal. En plus des caractéristiques vocales et de langage, Nuance peut détecter et analyser les caractéristiques de l'appareil (DeviceID) et du réseau (ChannelID) utilisés pour l'appel téléphonique. Une empreinte unique peut être créée pour identifier l'appareil d'un fraudeur (DevicePrint). Hormis la détection des caractéristiques audio d'un appel, Nuance permet aussi de détecter les comportements frauduleux, par exemple l'utilisation de robots, d'outils automatisés et de schémas d'appel.

De plus, Nuance détecte toutes les usurpations courantes par téléphone, notamment les voix enregistrées, les conversions de texte en voix (voix synthétiques) et l'usurpation de numéro de téléphone (identification automatique du numéro détournée). Sur les canaux digitaux, Nuance aide à détecter la fraude sur les nouveaux comptes et les piratages de comptes. D'après les schémas d'interaction de l'utilisateur avec l'appareil, Nuance détecte s'il s'agit d'un humain ou d'un robot et si le comportement est frauduleux ou conforme aux caractéristiques de l'utilisateur légitime. Nuance permet aussi de détecter toute activité suspecte au cours de la session, par exemple robots, accès à distance, utilisation de VPN ou d'adresses IP douteuses ou d'autres caractéristiques de risque.

Orchestration : Nuance permet d'orchestrer la logique métier sous-jacente aux processus d'enregistrement, d'authentification et de détection des fraudes ; l'interaction entre la solution et l'infrastructure du client ; et les intégrations à des systèmes tiers dans l'environnement client.

Facteurs biométriques : biométrie vocale, faciale, digitale (permet d'intégrer les résultats de capteurs d'empreintes digitales tels que Touch ID), comportementale.

Facteurs comportementaux : ConversationPrint est une technologie pour laquelle une demande de brevet a été déposée et qui analyse les schémas de langage pour authentifier l'utilisateur et détecter les fraudes. De plus, Nuance dispose d'une gamme de détecteurs comportementaux applicables aux canaux vocaux et de chat, par exemple pour détecter frappe, stylet et texte.

Facteurs propres au canal : possibilité de déterminer l'appareil et le modèle utilisés pendant une interaction ainsi que tout changement ou anomalie dans la manière dont l'utilisateur se sert de l'appareil. Détermine si l'appareil a changé afin d'indiquer un appel ou une session web/mobile potentiellement frauduleux. Analyse les métadonnées dans une interaction pour identifier les incohérences et déterminer une usurpation potentielle (c'est-à-dire numéro de téléphone usurpé). Détecte la position géographique grâce au réseau téléphonique et les anomalies de réseau sur tous les appareils, par exemple modification d'adresse IP et accès à distance.

Détection des fraudes (listes noires) : Nuance dispose de fonctionnalités de détection des fraudes en temps réel et hors ligne qui permettent de créer et de gérer des listes noires. Une liste noire peut contenir à la fois des empreintes biométriques, comportementales et celles d'un appareil. Une liste noire peut donc inclure des empreintes vocales, des empreintes conversationnelles (ConversationPrints), les empreintes d'un appareil (DevicePrints) et d'autres métadonnées comme le sexe, la langue parlée, ainsi que d'autres caractéristiques permettant de prioriser les alertes. La plateforme Nuance DataShare est un portail de partage d'informations qui permet aux participants de partager avec d'autres entreprises des données sur les individus ayant commis ou tenté de commettre une fraude à l'encontre d'une ou de plusieurs sociétés (le « service DataShare »).

Orchestration : Nuance permet d'orchestrer la logique métier qui sous-tend les processus d'enregistrement, d'authentification et la prise de décisions. La confiance dans l'identité revendiquée peut se fonder sur plusieurs couches de sécurité, notamment des facteurs biométriques et d'autres signaux de risque ou de familiarité.

Interface côté agent : l'interface utilisée par les agents affiche le statut et le résultat de l'authentification. Elle ne requiert aucune action de la part de l'agent ou de la personne qui interagit avec lui. Dans l'interface standard prête à l'emploi, les résultats s'affichent sous forme de réponses simples à comprendre, avec un code de couleurs, par exemple vert pour une authentification réussie, rouge pour un échec d'authentification et violet pour la détection d'un fraudeur. De plus, l'interface peut afficher d'autres métadonnées concernant l'appelant, notamment la classification de la voix, l'identification automatique du numéro et toute autre métadonnée utile pour l'agent.

Gestion d'un cas d'analyse/d'investigation : la fraude peut être détectée et signalée de deux manières. Dans le premier cas, les agents sont avertis en temps réel lorsque la voix de l'appelant correspond à l'empreinte vocale d'un fraudeur connu (liste noire). Les agents peuvent prendre immédiatement les mesures nécessaires. Nuance dispose également de fonctionnalités hors ligne qui permettent aux analystes d'enquêter sur une fraude potentielle après les faits (clustering des appelants et recherche en amont, par exemple).

Mise en œuvre

Modèle de livraison : direct et par le biais de partenaires
Principaux partenaires : Avaya, Cisco, KCOM, Genesys, Carahsoft, Accenture, Telstra, Diagenix, Vodafone, Deloitte Presidio
Gestion du service : fournit un service hébergé dans le cloud ; les déploiements dans un cloud privé seront pris en charge début 2021.
Taille de l'équipe des services professionnels : 700 personnes à l'échelle mondiale
Tarifs : tarification par paliers, en fonction du volume, à la transaction – permet d'adapter le prix selon la taille et le volume des déploiements
IAuth et propriété intellectuelle : 1 450 employés en R&D, +3 000 brevets

Plans et vision pour l'avenir

Fournir une authentification et une prévention des fraudes simples, efficaces et précises en continu grâce à la biométrie, sur tous les appareils et canaux d'interaction. D'ici 5 ans, l'authentification basée sur des connaissances aura disparu. Nuance proposera une solution de sécurité complète couvrant tous les besoins d'authentification et de prévention des fraudes dans l'entreprise et continuera à investir dans la recherche, notamment le développement de technologies anti-usurpation novatrices afin de garder une longueur d'avance sur les menaces émergentes.

Principaux critères de différenciation :

- Solution intégrée et complète d'authentification et de prévention des fraudes pour les canaux digitaux et vocaux, qui fournit une expérience client de bout en bout, avec traitement biométrique tant sur l'appareil que côté serveur.
- Meilleurs taux d'authentification réussie et de prévention des fraudes du secteur, fruit d'un investissement continu dans des technologies clés (réseaux de neurones multicouches de 4e génération, entre autres). En particulier, Lightning Engine permet une authentification indépendante du texte dans le SVI, avec une précision remarquable à partir d'énoncés très courts.
- Les clients obtiennent un meilleur ROI que les entreprises déployant des solutions concurrentes, davantage d'économies en termes de pertes liées à la fraude et un taux supérieur d'authentifications réussies.
- Transparence : toutes les vérifications sont accessibles aux clients afin d'expliquer la raison détaillée du résultat de l'authentification (bien mieux que l'approche basée sur liste noire).

SYMNEX

À propos de SymNex Consulting

SymNex Consulting aide des entreprises innovantes et orientées client à démontrer le bien-fondé d'une transformation de l'expérience d'accueil par téléphone, à concevoir cette transformation et à la mettre en œuvre. Ses services donnent des résultats remarquables en termes d'efficacité, de sécurité et de commodité des processus grâce à la technologie, au pragmatisme et à la compréhension des comportements.

À propos d'Opus Research

Opus Research est un cabinet de conseil et d'analyse diversifié qui fournit des informations clés sur les logiciels et services utilisés pour assurer un service client multimodal et améliorer l'expérience client. Opus Research est axée sur le « commerce conversationnel », à savoir la fusion entre technologies d'assistant intelligent, intelligence conversationnelle, authentification intelligente, collaboration d'entreprise et commerce numérique. www.opusresearch.net

Pour toute demande de renseignement concernant les ventes, veuillez contacter info@opusresearch.net ou appeler le +1(415) 904-7666