Autenticación Inteligente y Prevención de Fraude

Soluciones para las nuevas amenazas de seguridad y los retos de la experiencia del cliente »

opusresearch

opusresearch | Informe »

Autenticación Inteligente y Prevención de Fraude

Soluciones para las nuevas amenazas de seguridad y los retos de la experiencia del cliente »

En este nuevo informe, Opus Research y SymNex Consulting ofrecen a los responsables de negocio un análisis de mercado basado en la evaluación de distintos proveedores de soluciones, creadas para ofrecer experiencias de cliente seguras y prevenir el fraude. La autenticación inteligente (en adelante, «IAuth») incluye una serie de productos y servicios que van más allá de la biometría de voz e incluyen otros factores biométricos (facial, dactilar, comportamiento), prevención y detección del fraude y nuevos modelos de autenticación desde la aparición de los canales digitales. En este informe se evalúan 20 empresas, tanto proveedores de plataformas como proveedores de tecnología, con el fin de entender la variedad de soluciones que existen en el mercado y la habilidad los proveedores para seguir creando soluciones más completas y que respondan a las nuevas amenazas de seguridad y a los retos de la experiencia del cliente.

»

Agosto de 2020

Dan Miller, analista líder y fundador, Opus Research
Matt Smallman, director, SymNex Consulting
Derek Top, director de investigación, Opus Research

SYMNEX

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

www.opusresearch.net

» Índice

La autenticación es el primer paso en cualquier empresa 4
Acelerando el camino hacia la madurez 4
Evolución de la Autenticación de clientes 4
Foco en la IAuth y la Detección del Fraude 6
Conjunto de herramientas de autenticación 7
Conjunto de herramientas para la prevención de fraude 7
Orquestación 7
Dos categorías de respuestas 8
Criterios de evaluación de la IAuth 10
No pierdan de vista las nuevas soluciones inteligentes para la autenticación 10
Análisis de proveedores de plataformas y tecnología 11
Nuance – Perfil del proveedor 15

INFORMACIÓN DE LOS GRÁFICOS

Figura 1: Fases de la evolución de la autenticación 5
Figura 2: Definiendo el conjunto de herramientas de la autenticación inteligente 6
Figura 3: Empresas incluidas en el informe 9
Figura 4: Análisis de proveedores de plataformas en 2020 12
Figura 5: Análisis de proveedores de tecnología base en 2020 13
Figura 6: Análisis de ambos proveedores de soluciones de IAuth 2020 14

La autenticación es el primer paso en cualquier empresa

«No hay una segunda oportunidad para causar una primera buena impresión» era el eslogan publicitario de un fabricante de trajes masculinos en la década de 1960. Esta frase cobra un nuevo significado y relevancia hoy en día, ya que cada vez más conversaciones comerciales tienen lugar durante un período concreto a través de distintos dispositivos. Después de buscar en la web, consultar referencias de confianza en las redes sociales y visitar tiendas *online*, lo último que quiere un cliente o un cliente potencial es tener que recordar una contraseña o encontrar respuestas a «preguntas de seguridad».

Durante décadas, multitud de delincuentes se han aprovechado de la debilidad de los *contact centers* para acceder a información personal de los clientes, robar sus datos y cometer estafas relacionadas con el robo de bienes, servicios y dinero. Hace mucho tiempo que los procesos de autenticación han sustituido al «¿En qué puedo ayudarle?» como primer paso habitual (o, mejor dicho, obstáculo) en los departamentos de atención al cliente. La seguridad se impuso ante la experiencia de cliente y los procesos comenzaron a ser largos, molestos e ineficaces. Algunas de las prácticas más populares incluían el envío por SMS de contraseñas de un solo uso (OTP) y la autenticación basada en conocimiento (KBA). Hoy en día, se sabe bien que el primer método es vulnerable a los conocidos ataques "man in the middle", y el segundo depende en gran medida de información que los delincuentes pueden recopilar fácilmente de fuentes que están disponibles públicamente, como las redes sociales.

Opus Research define el término «autenticación inteligente» (IAuth) como una gama de soluciones y ofertas que han evolucionado desde la autenticación por voz para incluir otros factores biométricos (faciales, dactilares y conductuales), prevención y detección del fraude, y nuevos modelos de autenticación desde la aparición de los canales digitales.

Acelerando el camino hacia la madurez

Desde sus comienzos, las iniciativas de autenticación del cliente se centraban solamente en usar una breve lista de factores que dejaran fuera a los malos y permitieran a los clientes validados llevar a cabo sus actividades deseadas. Los PIN y las contraseñas (elementos de conocimiento; "algo que el cliente sabe") continuaron usándose y se añadieron a ellos molestas preguntas de seguridad y otras formas de autenticación basada en el conocimiento (KBA). Con demasiada frecuencia, eran los propios clientes quienes debían sufrir la tarea de recordar las contraseñas, responder a las preguntas de seguridad o introducir una contraseña de un solo uso que llegaba a través de un teléfono móvil o que encontraban en una «llave electrónica» proporcionada por la empresa.

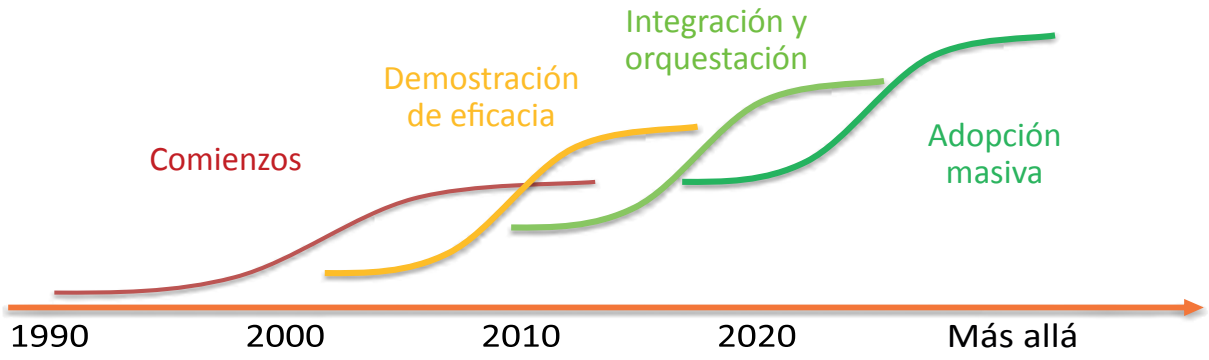
Las soluciones actuales tienen que hacer mucho más. Recuerde: ningún cliente llama ni se conecta a internet para autenticarse; su objetivo es otro, y la autenticación es un mal que tienen que padecer. Las soluciones actuales deben tener en cuenta el contexto, es decir, conocer la ubicación del cliente, la actividad anterior, el historial de transacciones e intención actual para poder encontrar el nivel de riesgo que deben asignar a ese cliente o actividad en particular. No deben suponer ningún esfuerzo o suponer un esfuerzo mínimo para el cliente mientras este trata de establecer comunicaciones de confianza con la empresa. Las empresas que facilitan un registro pasivo, que puede tener lugar durante el transcurso de una conversación con una IVR conversacional, asistente virtual o agente físico, son las que consiguen puntuaciones más altas en nuestra evaluación.

Evolución de la Autenticación de clientes

Las soluciones de IAuth (tanto en plataformas como en tecnologías básicas) apoyaron y evolucionaron al mismo tiempo que la transformación digital, los asistentes inteligentes y la IA conversacional. Es algo que comenzó lentamente a principios de este siglo, mientras se lidiaba con la preocupación de la precisión

y la rentabilidad. [En la figura 1 a continuación se muestra la evolución de la autenticación inteligente.] La adopción y la implementación se aceleraron de forma considerable a medida que la aceptación del usuario final quedó demostrada con los primeros en adoptarla (jóvenes adolescentes) y continuó acelerándose al demostrarse el retorno de la inversión.

Figura 1: Fases de la evolución de la autenticación



Factores	**Factor único (por ej., voz)**	**2FA**	**Multifactor**	**Continuidad**
Obstáculos para la adopción	**Precisión**	**Aceptación del usuario final**	**ROI**	**Ninguno**
Contexto	**IVR automatizada**	***Contact centers***	**Aplicaciones del lenguaje natural**	**Paso a la nube**
Productos y servicios	**Autenticación por voz en función del texto**	**Registro y autenticación activa y pasiva**	**Autenticación por capas, conocimiento del riesgo y detección del fraude**	**Autenticación continua, sin esfuerzo y detección del fraude pasiva**

- **Comienzos** (2000-2010): Con el enfoque «Mi voz es mi contraseña», los clientes que llamaban por teléfono sabían que usaban su voz (algo propio) en lugar de un PIN o contraseña (algo que saben). Las soluciones eran rígidas (en función del texto) e inducían a sospechas, sobre todo entre los profesionales de seguridad que trataban de evitar «falsos positivos».

Prueba de la eficacia (2011-2017): los proveedores de soluciones integraron con éxito mil millones de huellas de voz en sistemas para bancos, empresas de telecomunicaciones, proveedores sanitarios e instituciones públicas para acelerar la autenticación y disuadir el acceso fraudulento. La detección de estafadores en tiempo real usando varias tecnologías, como las redes neuronales profunda (DNN) además de la biometría de voz pasiva, tuvo un papel importante a la hora de justificar la inversión.

Integración y orquestación (2018-2020): los profesionales de experiencia del usuario (UX), seguridad y arquitectura informática colaboran con el personal de operaciones del *contact center* para integrar una variedad de biometría, motores de riesgo, diseño UX y otras plataformas de gestión del flujo de trabajo en soluciones del mundo real. Todos ellos reconocen el valor de la autenticación en tiempo real para mejorar las iniciativas de seguridad, experiencia del cliente y personalización.

Adopción masiva (aspiración): la solución creada por las empresas evaluadas en este documento amplió el atractivo al satisfacer la demanda del mundo real de una autenticación sólida y continua con estrategias de acceso al mercado que la hacen asequible para todas las empresas que tienen una relación duradera con sus clientes. En un mundo postpandémico, esto quiere decir que existen grandes oportunidades para el e-commerce, el sector sanitario con la telesalud y empresas públicas además de la banca, finanzas y telecomunicaciones.

Perspectiva de los clientes

«El proyecto comenzó en abril de 2016 con el objetivo de mejorar la seguridad, acortar el tiempo de gestión de las llamadas y reducir las incómodas preguntas de seguridad de los procesos de autenticación… Muchas de las dificultades tenían que ver con aspectos legales debidos a la protección de datos y las preguntas sobre aceptación o no aceptación… Tras algunos ajustes, se podía contar con un argumento comercial».

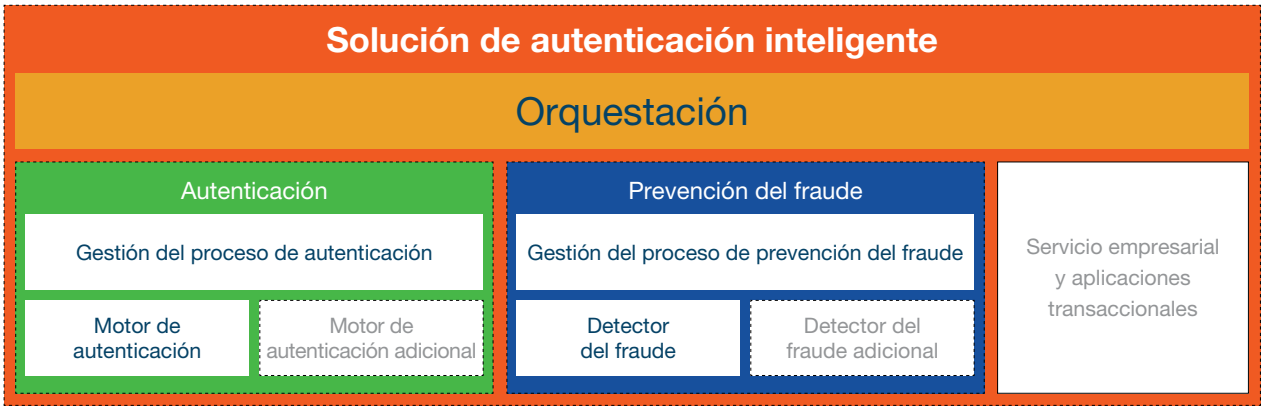
— Banco global con 2,5 millones de clientes particulares, 300 000 clientes de empresas y 500 agentes en el *call center*

Foco en la IAuth y la Detección del Fraude

Una solución de IAuth completa integra capacidades de autenticación y detección del fraude en la tecnología subyacente de los distintos canales, en los procesos necesarios para permitir la autenticación (como el registro y verificación) o en la detección del fraude (como una lista de seguimiento o gestión de casos), además de entre todos estos elementos para ofrecer un servicio al cliente seguro. En muchas empresas, este conjunto de herramientas, consistirá en una mezcla de soluciones personalizadas o en paquetes de distintos proveedores y de capacidades desarrolladas internamente. En la figura 2 a continuación, detallamos las capas y componentes conceptuales de este conjunto de herramientas para que los lectores puedan exponer sus requisitos con mayor claridad.

A medida que el mercado de la autenticación inteligente ha madurado en los últimos años, hemos observado el desarrollo de distintas áreas de orientación de los proveedores y de interés de las empresas. Los proveedores pueden elegir especializarse en una o dos «tecnologías base» para apoyar las necesidades o requisitos de los desarrolladores de aplicaciones con soluciones integradas. Otra categoría de proveedores adopta una visión holística más en línea con nuestra definición de IAuth y adecuada para abordar u orquestar un completo abanico de funciones de autenticación y detección del fraude.

Figura 2: Definiendo el conjunto de herramientas de la autenticación inteligente



FUENTE: Opus Research (2020)

Conjunto de herramientas de autenticación

El conjunto de herramientas de autenticación (en verde en la figura anterior) está formado por dos componentes principales de interés para los usuarios.

- Gestión del proceso de autenticación – Esta capa ofrece a la empresa características orientadas al usuario que son necesarias para que se usen uno o más motores centrales en un proceso de autenticación, como la gestión del consentimiento del usuario, el registro y la verificación. En muchos casos, los componentes de la autenticación solo exponen una API que puede usar la organización del usuario final o el integrador de los sistemas para desarrollar este componente.

- Biometría u otro motor de autenticación – El componente de autenticación lleva a cabo la correspondencia de patrones entre los datos que llegan en ese momento y las plantillas almacenadas. En el contexto del servicio al cliente, a menudo se trata de una biometría conductual o física, pero también puede incluir procesos de autenticación basados en el conocimiento. Además de establecer la correspondencia de los patrones, debe protegerse a sí mismo de vulnerabilidades conocidas, con la detección de mecanismos de falsificación (anti-spoofing) o detección de presentación de ataques.

Conjunto de herramientas para la prevención de fraude

El conjunto de herramientas para la prevención del fraude está también formado por dos capas de interés:

- Gestión del proceso de prevención del fraude – Esta capa es en la que se usan las alarmas de uno o más detectores para evaluar el riesgo de fraude de las interacciones y activar las acciones necesarias, bien en forma de gestión de casos o mediante la comunicación con otras aplicaciones.

- Detector del fraude – Este es el componente que interpreta la señal recibida del canal para ofrecer resultados comprensibles, como la detección de anomalías en audio, características de señalización o la correspondencia de firmas de agentes maliciosos conocidos.

Orquestación

El término «orquestación» se refiere a menudo al uso de la automatización, algoritmos o reglas para configurar, gestionar y coordinar sistemas informáticos, aplicaciones y servicios. Más concretamente, puede referirse a recursos que automatizan un proceso o flujo de trabajo con muchos pasos a través de múltiples sistemas. En el contexto de la IAuth, la orquestación coordina los procesos de autenticación y prevención del fraude usando un contexto adicional de otras aplicaciones de servicio o transaccionales de la empresa para determinar si se permite que las interacciones o transacciones continúen con o sin pasos adicionales de autenticación o prevención del fraude. Esto se basa normalmente en una «puntuación de riesgo» que en muchos casos gobierna cómo debe tratar una empresa a una persona concreta o la tarea que está llevando a cabo.

Las capacidades de orquestación son a menudo una fuente de diferenciación para los proveedores de plataformas de IAuth completas. Un grupo relativamente pequeño de proveedores de soluciones cuenta con ofertas que van más allá de la autenticación, prevención del fraude y orquestación. A través de conectores o API, incorporan información de bases de datos asociadas a otras aplicaciones o servicios que pueden gobernar la evaluación de un riesgo percibido y las acciones que deben emprenderse con base en esas evaluaciones.

Perspectiva de los clientes

«El mayor reto es producir un sistema escalable y seguro que pueda implementarse y puedan utilizar con facilidad las empresas y los consumidores… [La solución] sustituye a toda la autenticación con una comprobación biométrica de voz y facial que gestiona el sistema antes de la conexión con un agente, lo que ahorra a este tiempo en la llamada y mejora la seguridad».

—Director comercial de una empresa de seguridad de la información del Reino Unido

Dos categorías de respuestas

«¿Quiero una plataforma de un solo proveedor o las mejores tecnologías?» es una pregunta continua que acompaña al personal del *contact center*, responsables de la experiencia del cliente (CX) y profesionales de la seguridad, Project managers y departamentos de comprar, independientemente del sector, industria o del tamaño de la compañía.

Perspectiva de los clientes

[Para seleccionar al proveedor, queríamos] una solución de biometría de voz que estuviera en el mismo conjunto de aplicaciones que el sistema de grabación de voz y la herramienta de gestión de personal… [Era importante] que los usuarios accedieran fácilmente a un solo sistema.

—Empresa de servicios bancarios y financieros de Asia-Pacífico

Para preparar este documento, Opus Research llevó a cabo la evaluación de productos y servicios de IAuth de 20 proveedores: 7 proveedores de plataformas y 13 proveedores de tecnología base que facilitan la autenticación inteligente (IAuth) y la detección del fraude. Forman parte de las amplias áreas de oportunidad que se muestran en la figura 2:

- **Proveedores de plataformas:** ofrecen soluciones llave en mano que facilitan el registro de huellas de voz y otros aspectos biométricos, autenticación activa o pasiva y detección del fraude. Amplían su oferta con variedades de análisis, aprendizaje automático y redes neurales profundas (DNN) que impulsan motores de riesgo y recursos para la detección del fraude. Un diferenciador crucial es la «orquestación», que hace uso de motores de decisiones para enviar datos a otros elementos de la plataforma con base en la evaluación de datos en tiempo real, como el riesgo de que una persona concreta sea quien dice ser, que esté en un lugar donde se supone que debe estar, y que use un dispositivo que se asocia a ella, además de que no existen otras anomalías.

- **Proveedores de tecnología base:** esta categoría describe a empresas que han contratado a personal y han invertido de forma continua en tecnologías que abordan la dificultad de una autenticación continua, sólida y sin fricciones para facilitar el comercio conversacional.

Figura 3: Empresas incluidas en el informe

En este documento (apéndice A) se ofrecen unos perfiles resumidos de las ofertas de cada empresa de IAuth y se las coloca en un «escenario de IAuth» en función de las fortalezas de sus productos y posiciones en el mercado.

Empresa	Categoría	Diferenciación
Aculab	Tecnología base	Seguridad y autenticación por API
Auraya Systems	Tecnología base	Especialista en biometría de voz
Biocatch	Aspirante	Biometría conductual, modelos de IA
Daon	Plataforma	Plataforma IdentityX, orquestación de autenticación multifactor
ID R&D	Tecnología base	Biometría de voz de tecnología punta + reconocimiento facial, detección en vivo
Interactions	Aspirante	Autenticación por voz integrada en una plataforma de agente virtual inteligente
Journey	Aspirante	Orquestación de autenticación «conocimiento cero», autenticación mutua
LumenVox	Tecnología base	ASR, TTS, biometría de voz y analítica del habla
NICE	Plataforma	Autenticación en tiempo real, prevención del fraude en tiempo real, exposición de estafadores continua con IA
Nuance	Plataforma	Mayor base de huellas biométricas de voz; aplicación de la IA en la prevención y detección del fraude y orquestación
Nuestar-Trustid	Tecnología base	*Call center* + digital
Omilia	Plataforma	Autoservicio conversacional
Phonexia	Tecnología base	BV, analítica del habla
Pindrop	Plataforma	Autenticación basada en riesgo; detección del fraude; incorporación de DNN
Sestek	Tecnología base	Tecnología de habla amplia; autenticación activa
Spitch	Tecnología base	BV básica, agente virtual
Verbio	Tecnología base	Biometría de voz y procesamiento del habla
Verint	Plataforma	Biometría de voz y conductual para autenticación y fraude
VBG	Tecnología base	Especialista en biometría de voz; modelo SaaS; API
VoiceIT	Tecnología base	Facilidad de implementación de BV y diferenciadores API

Criterios de evaluación de la IAuth

Para facilitar las conversaciones con un fin entre las empresas y sus clientes, las primeras deben saludar y tratar a quienes llaman, a los visitantes o las interacciones de forma diferente. Para ello, ahora pueden aplicar una autenticación basada en el análisis predictivo, redes neuronales profundas y biometría (dactilar, voz, facial, conductual) para establecer las identidades y continuar con la transacción.
El objetivo de esta combinación de tecnologías es la autenticación inteligente y la prevención del fraude.

En este documento, Opus Research y SymNex Consulting evalúan a las empresas seleccionadas teniendo en cuenta los atributos siguientes:

- Tiempo real
- Contexto del riesgo
- Flexibilidad
- Multifactor – incluida la biometría conductual
- Multicapa

Todas las empresas analizadas se distinguen por la calidad de su oferta de servicios. Sin embargo, para ayudar a los lectores a seleccionar a un proveedor, no deben someterse a criterios de evaluación idénticos.

En resumen, los proveedores de plataformas reciben mayor puntuación por la exhaustividad de su oferta y por su habilidad para orquestar el rendimiento de una variedad de capacidades que permiten una autenticación sin fricciones. Por otro lado, los proveedores de tecnología base reciben mayor puntuación cuando invierten en tecnologías únicas y diferentes, además de en conectores, APIs y adoptan un enfoque de mercado que es flexible y facilita su incorporación en soluciones más amplias que responden a las nuevas amenazas de seguridad y a los retos de la experiencia del cliente.

No pierdan de vista las nuevas soluciones inteligentes para la autenticación

No pertenecen a ninguna categoría; son cambiantes.

Prestamos especial atención a tres empresas que se incluyen en esta evaluación a pesar de que sus ofertas de productos y servicios no entran dentro de las categorías de «plataforma» ni «tecnología base». Opus Research las considera líderes o proveedores de tecnología punta que potencian el concepto de IAuth, aunque no hay ninguna base para la comparación directa con otras empresas en sus respectivas categorías. Han creado una serie de servicios formidables que combinan los principios de la IAuth con un subconjunto de componentes de la solución general.

Journey.ai
Journey.ai ofrece una «plataforma de identidad de confianza» para solventar las carencias específicas de la infraestructura digital que facilita el comercio conversacional, equilibrando seguridad, privacidad y experiencia del cliente en distintos canales. Su enfoque de «confianza cero» permite a las empresas usar sus aplicaciones y teléfonos móviles para registrar a clientes y agentes y usar después sus recursos para utilizar una serie de factores de autenticación, incluida la biometría, de forma flexible. Aplica técnicas novedosas a lo que llama «autenticación mutua» e incluye biometría conductual como parte de la mezcla de los factores de autenticación para facilitar una experiencia continua y sin fricciones.

BioCatch
BioCatch ofrece tecnología biometría conductual base para crear perfiles basados en acciones, como el movimiento del ratón, rapidez al teclear, patrones de deslizamiento u orientación del dispositivo que, cuando se comparan con los perfiles del nivel poblacional, pueden detectar a estafadores o impostores. Para los bancos, empresas de seguros y emisores de tarjetas de crédito es una herramienta importante para prevenir el fraude con «cuentas nuevas» y detectar a impostores, bots y el uso de voces «sintéticas» para obtener acceso a cuentas existentes.

Interactions LLC
Incluimos Interactions porque ofrece una autenticación biométrica por voz demostrada y capacidades de detección del fraude como complemento natural al asistente virtual de voz más amplio de Interactions. No se comercializa como tecnología base independiente ni se integra en una plataforma de IAuth más amplia; se vincula a motores de riesgo y decisión. Opus Research cree que las empresas que usan los asistentes virtuales inteligentes de Interactions descubrirán que sus recursos de registro y autenticación son una alternativa que merece la pena evaluar.

Análisis de proveedores de plataformas y tecnología

Para ayudar a los responsables de la toma de decisiones a evaluar a los proveedores de soluciones, Opus Research representa su posicionamiento en distintos gráficos de forma visual. En los gráficos 4, 5 y 6 que se muestran a continuación, hemos colocado a los proveedores de soluciones conforme al posicionamiento y éxito en el mercado relativo. El tamaño de los óvalos refleja dos factores de gran importancia:

- **Plenitud/flexibilidad del producto** – Los proveedores de plataformas reciben la mejor evaluación de «plenitud» cuando los servicios y características abarcan todas las columnas de la pila de soluciones: autenticación, prevención del fraude, orquestación y aplicaciones. Los proveedores de tecnología base se valoran por la habilidad para integrarse en los proveedores de soluciones completas a través de conectores e interfaces de programación de aplicaciones (API).

- **Potencial estratégico** – Para los proveedores de plataformas y de tecnología base, esta métrica captura cómo la visión y hoja de ruta se adaptan a los requisitos tecnológicos actuales y en constante evolución, en el *contact center* y más allá. La habilidad para funcionar con múltiples factores, como la biometría conductual, e incorporar nuevas tecnologías, como las redes neuronales profundas, son una ventaja. También lo es la habilidad para funcionar con aplicaciones del IoT, terminales inteligentes y móviles. También se tiene en cuenta el ecosistema de partners para llegar al mercado de cada empresa, así como de sus integradores y desarrolladores.

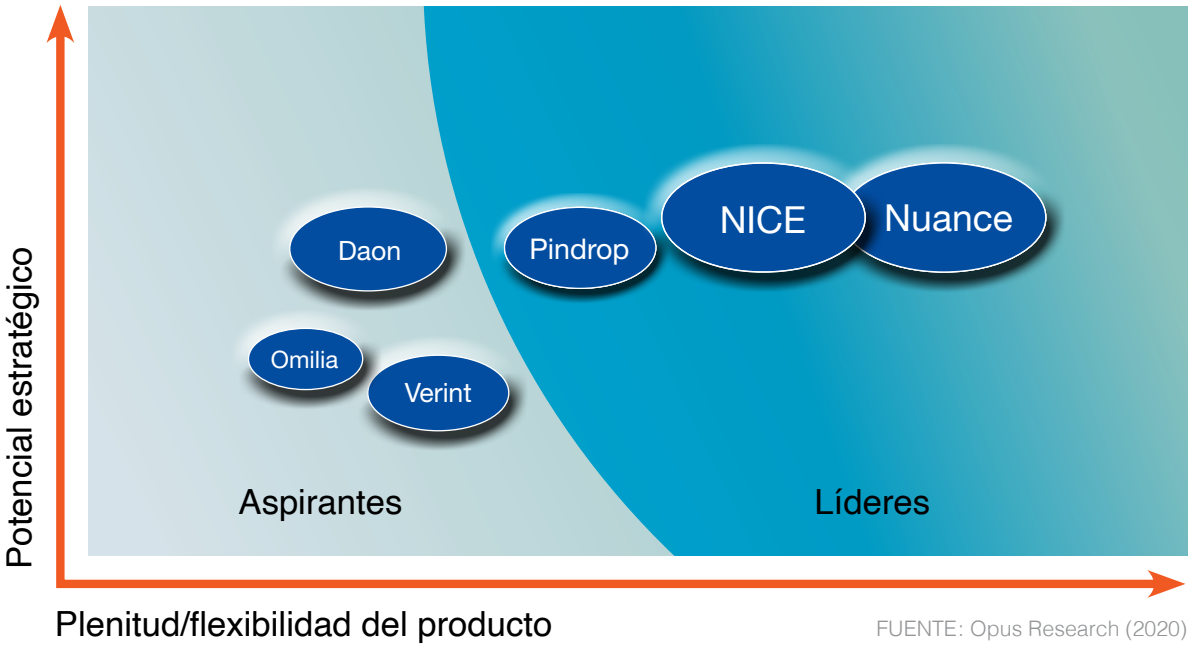
El tamaño de los óvalos representa la presencia de cada proveedor con base en la información proporcionada por la propia empresa o disponible públicamente sobre la fortaleza financiera actual (ingresos, rentabilidad, solvencia financiera, longevidad y tamaño de la base de clientes).

Los colores de los óvalos hacen referencia a la categoría del proveedor:

Proveedores de plataformas

Proveedores de tecnología base

Figura 4: Análisis de proveedores de plataformas en 2020

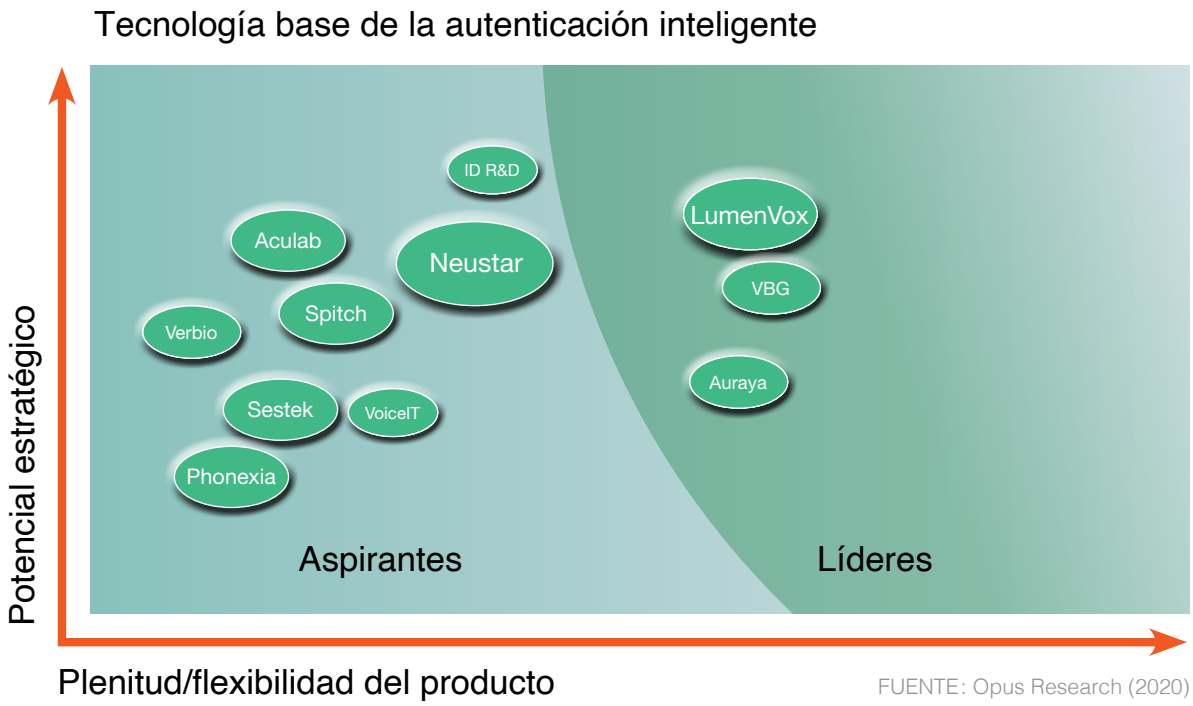


FUENTE: Opus Research (2020)

- Entre los líderes en proveedores de plataformas, destacan Nuance y NICE por sus tecnologías de autenticación integrales, ofertas integradas de prevención del fraude y bases de clientes sólidas y establecidas. Las soluciones incluyen Lightning Engine, ConversationPrint y DevicePrint de Nuance, y ENLIGHTEN Fraud Prevention en tiempo real de NICE, que aprovecha los modelos de comportamiento y análisis de voz con tecnología de IA para proporcionar información en tiempo real a los agentes.
- Pindrop se ha distinguido por su tecnología patentada para la verificación de riesgos, fraudes e identidad, aprovechando la autenticación basada en riesgos con acceso a una grande y completa base de datos de estafadores.
- Daon cuenta con implementaciones de producción a escala global que autentican millones de transacciones de identidad en multitud de autenticaciones biométricas.
- Verint tiene una amplia experiencia en interacción con el cliente y análisis del habla, y ha creado una nueva lista de clientes de autenticación y prevención de fraude.

- Omilia aprovecha la estrecha integración entre su motor de autenticación y la plataforma de IA conversacional para proporcionar una solución convincente a las empresas que buscan ambas cosas. Su motor de autenticación también está disponible como componente independiente.

Figura 5: Análisis de proveedores de tecnología base en 2020



FUENTE: Opus Research (2020)

- La fusión de LumenVox con VoiceTrust combina un proveedor de soluciones biométricas idóneo con el reconocimiento de voz establecido, relaciones con socios y experiencia de integración profunda de LumenVox. Voice Biometrics Group (VBG) y Auraya se centran en particular en la biometría de voz, y con millones de usuarios registrados, sus soluciones se benefician de esta madurez y enfoque profundo.

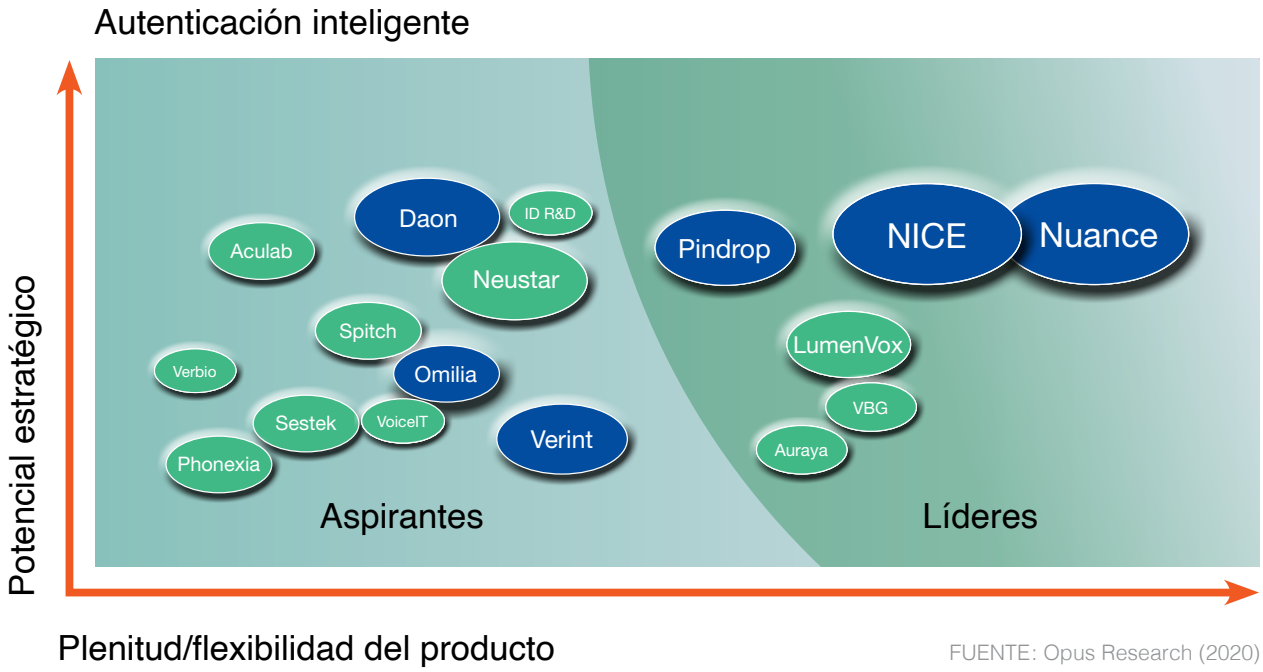
- ID R&D se ha centrado en casos de uso de aplicaciones y dispositivos móviles con resultados impresionantes de pruebas académicas y de la industria. Neustar, con la adquisición de TRUSTID, combina productos de distintos canales para casos de uso de autenticación y fraude digital y del *call center*.

- VoiceIt es una propuesta de servicio única para la que solo se necesita una tarjeta de crédito para comenzar. Proporciona código de muestra suficiente para que las principales plataformas que se desarrollen puedan ponerse en funcionamiento e implementar aplicaciones en horas en lugar de meses.

- Verbio y Spitch han desarrollado capacidades de biometría de voz junto con su cartera más amplia de tecnología de voz, tienen varias implementaciones y son verdaderos aspirantes en los mercados elegidos. Aculab aporta más de 40 años de experiencia en tecnologías de procesamiento de señales y telefonía para desafiar a los actores establecidos en el mercado de la biometría de voz.

- Sestek, con sede en Turquía, incluye la autenticación de voz con un amplio conjunto de soluciones conversacionales. Phonexia está llevando su experiencia gubernamental líder en el mercado al mercado comercial.

Figura 6: Análisis de ambos proveedores de soluciones de IAuth 2020



FUENTE: Opus Research (2020)

Nuance

Sede: Burlington, MA, EE. UU.
Año de fundación de la empresa: 1992
Ingresos: ~1500 millones de dólares
Número de empleados: ~8500

Alcance de los servicios de IAuth:

Ayuda en el proceso de registro e inicio de acceso a la cuenta: Facilita el registro de clientes a través de distintos canales. En todas las implementaciones, las personas que llaman pasan por un proceso de registro de voz, ya sea mediante una conversación natural con un agente en el caso de un *call center* (autenticación pasiva) o usando una frase a modo de contraseña (autenticación activa). En los canales digitales, el registro se puede activar a través de APIs de biometría de voz, comportamiento y facial.

Autenticación: Nuance ofrece una amplia variedad de métodos de autenticación que incluyen biometría de voz activa (en función del texto), biometría de voz pasiva (independiente del texto), validación de llamadas, ConversationPrint (elección de vocabulario, gramática y estructura de oraciones), DevicePrint (una huella única utilizada para identificar el dispositivo según la acústica y el canal), reconocimiento facial y biometría de comportamiento. Lightning Engine de Nuance permite la autenticación independiente del texto en la IVR, logrando una alta precisión con frases muy breves. Los detectores inteligentes proporcionan señales de familiaridad o riesgo para aportar confianza a la decisión de autenticación. Nuance también brinda la capacidad de agregar modalidades biométricas y no biométricas adicionales a través de complementos y un motor de riesgo incorporado para administrar los procesos de autenticación y detección del fraude a través de múltiples factores.

Prevención del fraude: Nuance ofrece la capacidad de detectar el fraude en los canales de voz y canales digitales, y una visión consolidada de la actividad de riesgo en todos los canales. Nuance puede detectar y analizar todas las características del fraude actualmente conocidas dentro del canal (voz y digital). Esto incluye la identificación de las características de voz de la persona que llama fraudulenta (biometría de voz), lo que permite la detección, identificación y posterior procesamiento del estafador en un tribunal de justicia con base en la evidencia biométrica.

Nuance puede detectar a un estafador a través de sus características del habla y su comportamiento, en particular, su elección de vocabulario, gramática y estructura de la oración (ConversationPrint). Nuance proporciona la única solución de prevención de fraude que identifica a un estafador con dos factores biométricos independientes en el canal de voz. Además de las características de voz y habla, Nuance puede detectar y analizar características producidas por el dispositivo (DeviceID) y la red (ChannelID) que se utilizan para realizar la llamada telefónica. Se puede crear una huella única para identificar el dispositivo de un estafador (DevicePrint). Más allá de detectar las características de audio en una llamada, Nuance también puede detectar comportamientos fraudulentos, como el uso de bots, herramientas automatizadas y patrones de llamadas.

Además, Nuance detecta todos los ataques de suplantación de identidad conocidos dentro del canal telefónico, incluidos los ataques basados en grabaciones (Playback Detection), los ataques texto-voz (detección de voces sintéticas) y los ataques a números de teléfono (detección de suplantación de identidad mediante ANI). En los canales digitales, Nuance puede ayudar a detectar el fraude de nuevas cuentas y la apropiación indebida de cuentas. Según los patrones de interacción del usuario con el dispositivo, Nuance puede detectar si se trata de un humano o un bot, si su comportamiento parece ser fraudulento o si es coherente con el comportamiento del usuario legítimo. Nuance también puede detectar actividad sospechosa en la sesión, como el uso de bots, sesiones de acceso remoto, el uso de VPN o IP poco fiables y otras características de riesgo.

Capacidad de orquestación: Nuance ofrece la capacidad de orquestar la lógica detrás de los flujos de registro, autenticación y detección del fraude; la interacción entre la solución y la infraestructura del cliente; y las integraciones con sistemas de terceros dentro del entorno del cliente..

Factores biométricos: voz, facial, dactilar (puede integrar resultados de sensores de huellas digitales, como Touch ID) y biometría conductual.

Factores conductuales: ConversationPrint es una tecnología pendiente de patente que analiza los patrones del lenguaje para la autenticación y la detección del fraude. Además, Nuance tiene una gama de detectores de comportamiento compatibles tanto para voz como texto/*chat*, capaces de detectar, por ejemplo, patrones en la forma de escribir, la manera de teclear y el tipo de texto.

Factores de canal: capaces de determinar el dispositivo y modelo utilizados durante una interacción, así como los cambios y anomalías en la forma en que el usuario utiliza un dispositivo. Determinan si el dispositivo ha cambiado para indicar una posible llamada o sesión web/móvil fraudulenta. Analizan los metadatos en una interacción para identificar incoherencias y determinar la posible suplantación de identidad (es decir, un número de teléfono falso). Detecta la ubicación geográfica a través de la red telefónica y las anomalías basadas en la red de todos los dispositivos, como el cambio de IP y las sesiones de acceso en remoto.

Detección del fraude (listas de vigilancia o watchlists): Nuance tiene capacidades de detección de fraude en tiempo real *offline* que permiten la creación de alertas y la gestión de listas de vigilancia. Una lista de vigilancia puede contener huellas biométricas, de dispositivos y de comportamiento. Como tal, una lista de seguimiento puede incluir huellas de voz, huellas de conversación (ConversationPrint) y huellas del dispositivo (DevicePrint) junto con metadatos adicionales como el género, el idioma y otras características que pueden ser variables y que se pueden aprovechar para priorizar las alertas. La plataforma Nuance DataShare es un portal de intercambio de información de Nuance que permite a un participante compartir con otras organizaciones ciertos datos de personas que se sabe que han cometido o han intentado cometer un fraude contra una o más organizaciones (el «Servicio DataShare»).

Orquestación: Nuance puede orquestar la lógica del negocio en torno a los flujos de registro y autenticación y la toma de decisiones. La confianza en la identidad solicitada se basa en múltiples capas de seguridad, incluyendo factores biométricos y señales adicionales de familiaridad y riesgo.

Interfaz de usuario del agente: la GUI (Graphical User Interface) del agente muestra el estado y el resultado de la autenticación. La GUI no requiere ninguna acción por parte del agente ni de la persona que interactúa con el agente. En la GUI estándar, se muestran los resultados al agente en respuestas codificadas por colores fáciles de entender, como verde para una autenticación satisfactoria, rojo para una autenticación fallida y violeta para la detección de un estafador. Además, la GUI puede mostrar información adicional sobre la persona que llama, incluyendo su clasificación de voz, el código ANI (Identificación Automática del Número llamante) y cualquier otro metadato que pueda ser útil para el agente.

Gestión de casos de analistas/investigaciones: el fraude se detectará y notificará de dos formas. Por un lado, los responsables/analistas de fraude recibirán alertas y notificaciones cuando la voz de la persona que llama coincida con la huella de voz de un estafador conocido incluido en la lista de vigilancia en tiempo real. Hecho que permitirá que los responsables emprendan las acciones pertinentes de forma inmediata. Por otro lado, Nuance también tiene capacidades *offline* que permiten que un posible ataque de fraude sea investigado por analistas de fraude y abordado a posteriori. Estas capacidades *offline* ayudan a mejorar las listas de seguimiento y permiten un análisis más exhaustivo del caso mediante técnicas como el *speaker clustering* (agrupación y segmentación de voces de hablantes) y la búsqueda regresiva.

Implementación:

Modelo de entrega: tanto de forma directa como a través de los principales partners: Avaya, Cisco, KCOM, Genesys, Carahsoft, Accenture, Telstra, Diagenix, Vodafone, Deloitte, Presidio, etc.
Gestión del servicio: tanto en local como en la nube. Tamaño del equipo de **servicios profesionales:** 700 personas en todo el mundo. **Precio:** precios escalonados en base al volumen y número de transacciones. Esto permite que el precio se adapte a volúmenes y tamaños distintos de implementaciones. Propiedad intelectual de IAuth: 1450 empleados de I+D, más de 3000 patentes.

Visión y planes futuros

Proporcionar una autenticación y prevención de fraude atemporal, sencilla, eficiente y sin fricciones a través de la biometría, en distintos dispositivos y canales de interacción. En un plazo de 5 años, dejará de existir la autenticación basada en el conocimiento. Nuance ofrecerá una solución de seguridad integral para abordar todas las necesidades de autenticación y prevención del fraude de las empresas, y continuará invirtiendo en investigación, incluyendo el desarrollo de tecnologías novedosas contra la suplantación de identidad para adelantarse a las amenazas emergentes.

Diferenciadores clave:

- Soluciones de autenticación y prevención de fraude integradas en los canales digitales y de voz para brindar una experiencia de cliente de principio a fin, con procesamiento biométrico en el dispositivo y en el servidor.
- Tasa de éxito de autenticación e índice de prevención del fraude líderes en la industria, e inversión continua en tecnología base (incluida la 4.ª generación de DNN). Es importante destacar, el motor Lightning Engine que permite la autenticación independiente del texto en la IVR, logrando una alta precisión con frases muy breves.
- Los clientes de Nuance consiguen mayor ROI, una cifra de ahorro más elevada al evitar pérdidas por fraude, y una tasa de éxito en la autenticación más alta en comparación con las organizaciones que implementan soluciones de la competencia.
- Total transparencia, haciendo todas las comprobaciones necesarias para el cliente y poniendo a su disposición y conocimiento la razón detrás de cada autenticación.

SYMNEX

Acerca de SymNex Consulting

SymNex Consulting trabaja con algunas de las organizaciones más innovadoras y orientadas al cliente para ayudarlas a defender, diseñar e implementar cambios transformacionales en la experiencia de bienvenida telefónica. Ofrece mejoras sustanciales en la eficiencia, seguridad y conveniencia de estos procesos a través de la tecnología, el pragmatismo y la comprensión del comportamiento.

Acerca de Opus Research

Opus Research es una empresa de análisis de mercado y consultoría diversificada que brinda información crítica sobre software y servicios que respaldan la atención al cliente multimodal y la mejora de las experiencias del cliente. Opus Research se centra en el «comercio conversacional», la fusión de tecnologías de asistentes inteligentes, la inteligencia conversacional, la autenticación inteligente, la colaboración empresarial y el comercio digital. . www.opusresearch.net

Para cualquier consulta sobre ventas, escriba un correo electrónico a info@opusresearch.net o llame al +1(415) 904-7666