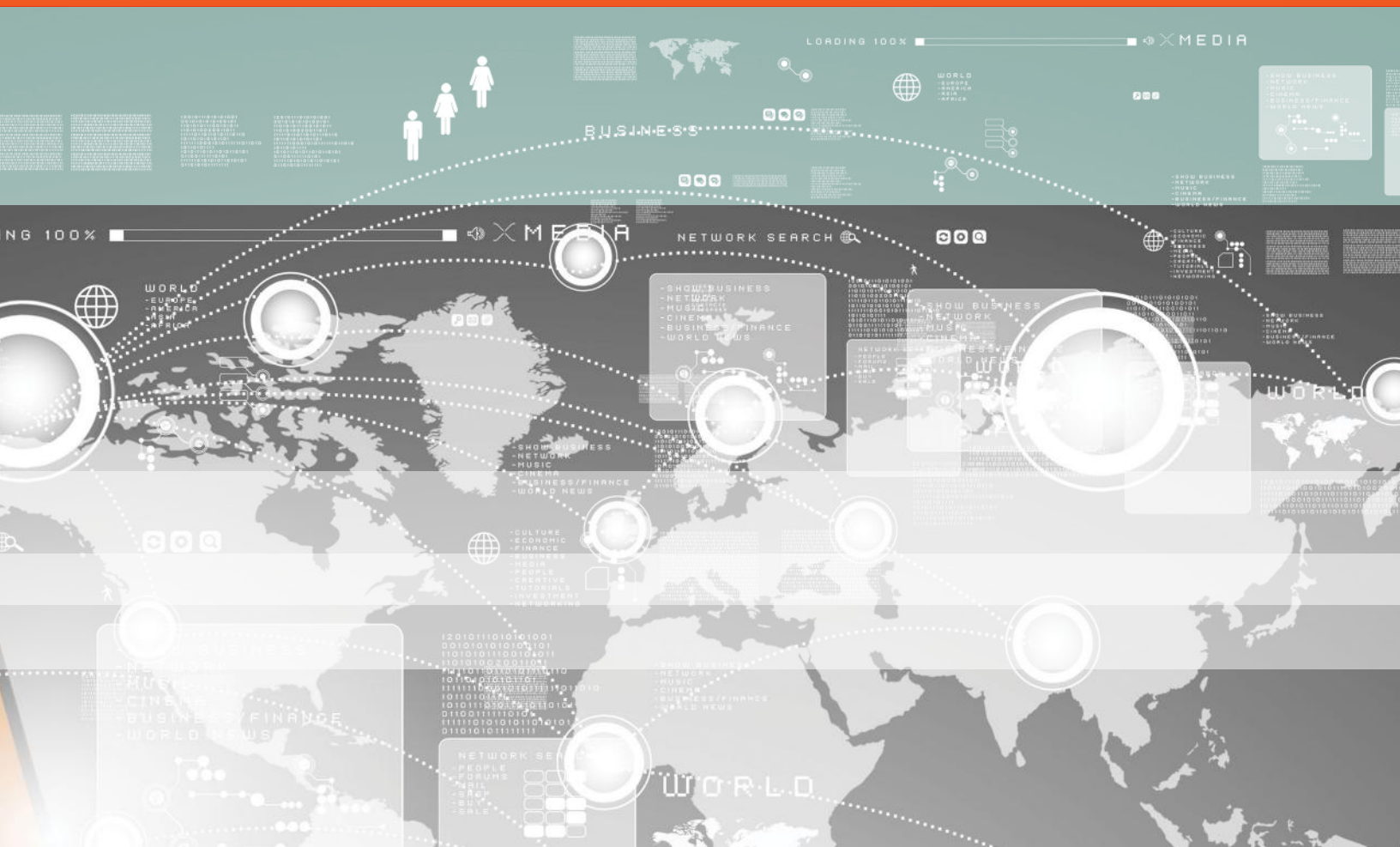
Autenticación Inteligente y Prevención de Fraudes - Intelliview 2022

opusresearch



opusresearch | Informe »

Autenticación Inteligente y Prevención de Fraudes - Intelliview 2022

En esta cuarta edición de Intelliview, Opus Research y SymNex Consulting proporcionan a los responsables de la toma de decisiones empresariales un contexto competitivo para evaluar a los proveedores de soluciones seleccionados que respaldan experiencias seguras de contacto con los clientes y la prevención de fraudes.

La autenticación inteligente (IAuth) captura una gama de productos y servicios que incluye factores biométricos (voz, facial, huella digital, comportamiento), inteligencia de red y orquestación utilizados para la detección de fraudes y la autenticación continua.

Este informe evalúa a 22 proveedores de soluciones de todo el espectro de IAuth que están implementando activamente tecnologías que mejoran la seguridad empresarial, la eficiencia y la experiencia del cliente.

Enero de 2022

Matt Smallman, Director, SymNex Consulting
Dan Miller, Fundador y Analista Principal, Opus Research
Derek Top, Director de Investigación, Opus Research

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

www.opusresearch.net

Índice

Índice de figuras

Resumen ejecutivo

Los requisitos para la autenticación inteligente (IAuth) han cambiado significativamente desde que Opus Research y SymNex Consulting emitieron nuestro último Intelliview. Miles de millones de personas, a menudo en confinamiento, utilizan habitualmente smartphones, tabletas o PC conectados para la banca, el comercio electrónico, la telesalud y para hacer uso de los servicios gubernamentales. Los impostores fraudulentos también han intensificado notablemente los esfuerzos para aprovechar las estrategias de autenticación vulnerables.

Los 22 proveedores de soluciones evaluados amplían el concepto de IAuth más allá de la autenticación de voz en centros de contacto o IVR para admitir el uso en tiempo real (a menudo pasivo) de múltiples factores biométricos, informados por la inteligencia de red y orquestados por motores de decisión infundidos por IA.

Las observaciones más importantes son las siguientes:

- **Las soluciones abordan la autenticación y la prevención de fraudes:** Las mismas tecnologías que permiten una autenticación sólida también se pueden implementar para la prevención de fraudes. La transición a la autenticación moderna lleva tiempo. Los enfoques con detección de fraude mejorada pueden ofrecer devoluciones inmediatas y mantener a los defraudadores a raya durante la transición.
- **Los smartphones juegan un papel en expansión:** Los micrófonos capturan la voz, las cámaras admiten el reconocimiento facial, pero eso es solo el principio. Los smartphones son dispositivos altamente personales que son compañeros constantes para sus propietarios. La posesión es un factor en sí mismo. La forma en que cada propietario de un smartphone ingresa información a través de una pantalla o pone el teléfono en su bolsillo puede ayudar a generar puntuaciones de confianza de que las personas son quienes dicen ser.
- **La biometría de voz es fundamental:** IAuth Intelliview comenzó con proveedores de soluciones que utilizaban biometría de voz para la autenticación de llamadas. El informe del año pasado incluyó empresas que agregaron biometría de comportamiento y asignaron importancia a los recursos que orquestan la combinación de factores que emplear en función del riesgo asociado con un individuo y sus acciones.
- **Emergencia de autenticación de red y detección de fraude:** La señalización y otros datos de inteligencia de red permiten la autenticación basada en posesión y la detección de anomalías para identificar llamadas potencialmente fraudulentas. La detección de fraude y el desvío de llamadas pueden tener lugar antes de que se involucre a un agente en vivo, poniendo la inteligencia de red a trabajar para establecer enlaces de comunicaciones seguros y confiables entre empresas y clientes.
- **La identificación del consumidor y la administración de acceso (CIAM) se quedan cortas:** Los proveedores de "IAM" de la vieja guardia abordan algunos de los desafíos de la seguridad digital y móvil y la autenticación de usuarios, como el registro/inscripción y el inicio de sesión único, pero solo ahora comienzan a abordar los problemas básicos de la experiencia de usuario que son de vital importancia para respaldar la autenticación continua y libre de fricción y la prevención de fraudes.
- **Espere más casos de uso verticales y de menor escala:** Las tecnologías básicas de IAuth han demostrado precisión, efectividad y retorno de la inversión a escala en sectores verticales sensibles como la banca, los seguros, el cuidado de la salud y el gobierno. Las soluciones ahora abordan tanto la seguridad como la personalización para minoristas, cadenas de restaurantes, farmacias y otras verticales con transacciones de menor volumen y menor valor.

Soluciones modernas para la autenticación y la prevención de fraudes

Ha llegado la hora de IAuth. Las empresas de todos los tamaños, en una serie de industrias verticales, han descubierto que sus métodos tradicionales de autenticación de clientes (principalmente PIN, contraseñas y preguntas basadas en el conocimiento) son insuficientes en términos de seguridad. Es más, los clientes encuentran que son incómodos, consumen mucho tiempo y son engorrosos. Los proveedores de soluciones evaluados en este Intelliview aportan tecnologías y enfoques modernos para identificar a los impostores y frustrar los intentos de fraude.

Sus servicios comienzan con motores biométricos que pueden emparejar la voz o las características faciales de una persona con plantillas almacenadas (huellas de voz o huellas faciales) para medir qué tan segura puede estar una empresa de que las personas son quienes dicen ser. Eso ha demostrado ser un buen comienzo, pero las soluciones de hoy en día agregan una variedad más amplia de factores biométricos, incluido el comportamiento, como la forma en que introducen información en un teclado.

Todo puede aumentarse con "Inteligencia de red" e "Inteligencia de dispositivo". La primera describe los conocimientos que se pueden obtener evaluando las señales que proporcionan las compañías telefónicas al completar las llamadas entre las empresas y sus clientes para garantizar que el número presentado sea el originador y, por lo tanto, asegurar la posesión frente al intercambio de SIM y la "suplantación". La segunda se centra en técnicas basadas en dispositivos, que pueden crear una clave aún más segura para la empresa, asegurando no solo que el usuario está en posesión de ese dispositivo, sino que realmente es su propietario.

Apelación a un espectro más amplio de negocios

Grandes bancos, casas de corretaje, compañías de seguros, proveedores de servicios inalámbricos e Internet y minoristas fueron los primeros en adoptar la autenticación basada en biometría de voz, el precursor de IAuth.

Según las estimaciones de Opus Research, las empresas evaluadas en este documento están asegurando cerca de 20 000 millones de interacciones al año con la biometría de voz. Además, los proveedores de soluciones biométricas de comportamiento han instalado software en más de 100 millones de dispositivos colectivos y, en conjunto, realizan algo del orden de otras 30 000 millones de transacciones de autenticación.

Los gigantes de los centros de contacto basados en la nube, incluidos Amazon Connect y Google Contact Center AI, están acelerando el conocimiento y la adopción de IAuth al incluirlo en sus ofertas de servicios.

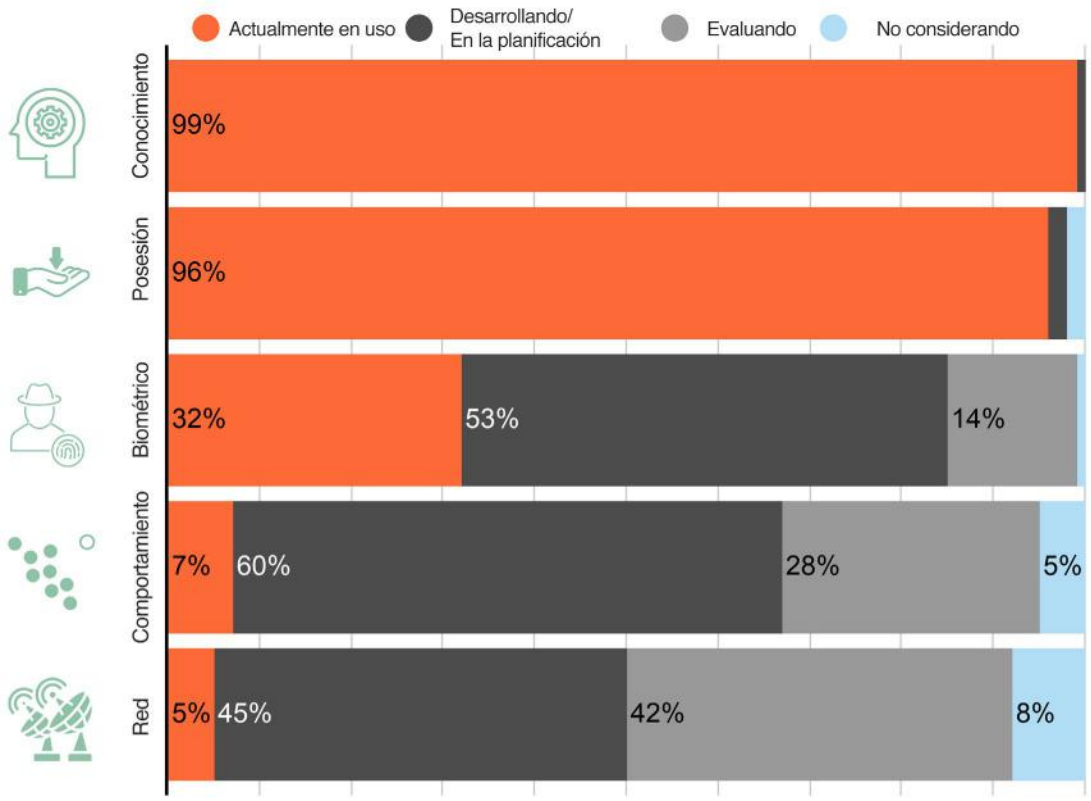
Los resultados de campo muestran un creciente interés en nuevos métodos de autenticación

Para comprender mejor el "Estado de la Autenticación Inteligente", Opus Research recientemente encuestó a 250 responsables ejecutivos de la toma de decisiones de múltiples industrias en los EE. UU., Canadá, Reino Unido y Europa Occidental sobre tecnologías empresariales para la seguridad, la autenticación y la prevención de fraudes.

Cuando se les preguntó qué métodos de autenticación y detección de fraude estaban utilizando las organizaciones, vemos una amplia gama de opciones y múltiples factores en uso. Los encuestados ya combinan un conjunto de soluciones de métodos de autenticación y prevención de fraudes.

Si bien los PIN/contraseñas siguen siendo los más comunes, los encuestados también incorporan otros factores, como la coincidencia de ANI, la entrega fuera de banda de contraseñas de un solo uso y la autenticación basada en el conocimiento a través de preguntas de seguridad. Un número creciente está adoptando la biometría de voz y comportamiento, y está adquiriendo un fuerte interés en el desarrollo y evaluación de soluciones de autenticación de red.

Figura 1: Métodos tecnológicos para la autenticación y detección de fraude

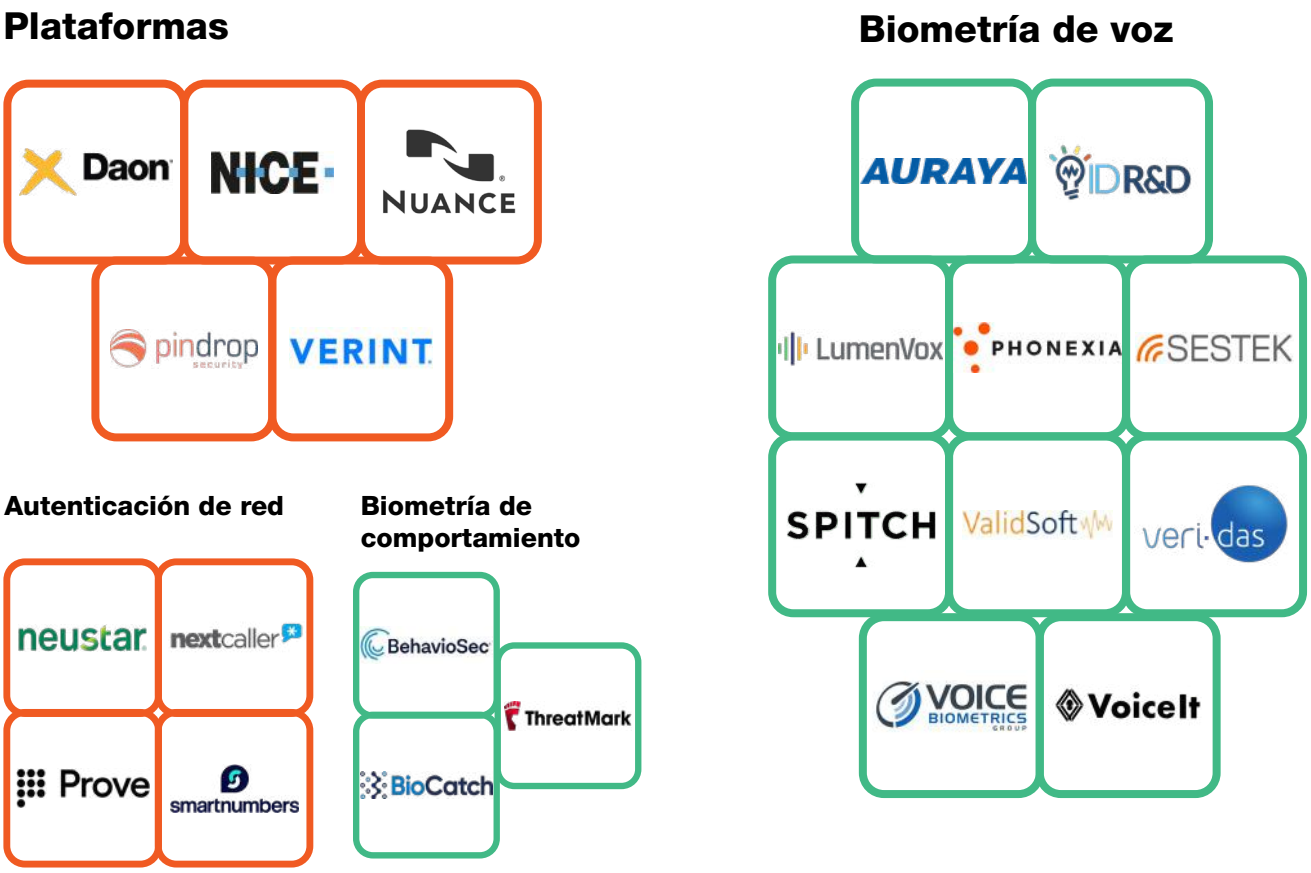


Empresas incluidas en el Intelliview

Las empresas incluidas en este informe no siempre compiten cara a cara en el mercado, pero cada una es digna de consideración ya que las empresas buscan proveedores de soluciones que apoyen sus estrategias para la autenticación continua y sin fricciones o la prevención de fraudes.

Este documento (Apéndice A) proporciona breves perfiles de las ofertas de IAuth de cada empresa y también las sitúa en un "paisaje de IAuth" basado en la solidez de sus ofertas de productos y posiciones en el mercado.

Figura 2: Proveedores de soluciones en evaluación



Innovación en biometría de voz

Autenticación independiente de texto de expresión corta

Anteriormente muchos proveedores competían por la precisión, pero vemos cada vez más que las diferencias de rendimiento de los proveedores son irrelevantes para los resultados empresariales del usuario final. Hemos visto cada vez más a los proveedores centrar sus esfuerzos en el rendimiento de la autenticación de expresiones cortas con independencia de texto.

Impulsado por la demanda de usar esta tecnología en IVR de comprensión del lenguaje natural sin frases de contraseña antinaturales y difíciles de inscribir donde las expresiones individuales de los clientes suelen ser de menos de dos segundos. Hoy en día, la mayoría de estas soluciones todavía requieren frases de inscripción mucho más largas, generalmente adquiridas durante las conversaciones con los agentes.

Sin embargo, algunos proveedores también están buscando longitudes de audio de inscripción más cortas para reducir los gastos generales de inscripción del agente. Por supuesto, con todo lo relacionado con la biometría de voz, puede que el equilibrio entre la longitud y el rendimiento no esté exactamente donde todos los usuarios finales quieren que esté, pero esperamos que esta sea un área de enfoque cada vez mayor en el próximo año.

"LA BIOMETRÍA DE VOZ YA HA EVITADO MÁS DE 1000 ADQUISICIONES DE CUENTAS Y NOS ESTÁ AHORRANDO MÁS DE 40 SEGUNDOS POR LLAMADA EN PROMEDIO"

–Director de Prevención de Fraudes, Corporación Bancaria Multinacional

---

Centro de contacto en la nube

El requisito impulsado por la pandemia de permitir el trabajo a domicilio ha acelerado la transición a centros de contacto en la nube para muchas empresas. Si bien la prioridad ha sido poner en marcha esos servicios con una interrupción mínima, vemos un número cada vez mayor de empresas que comienzan a aprovechar la mayor flexibilidad de estas soluciones.

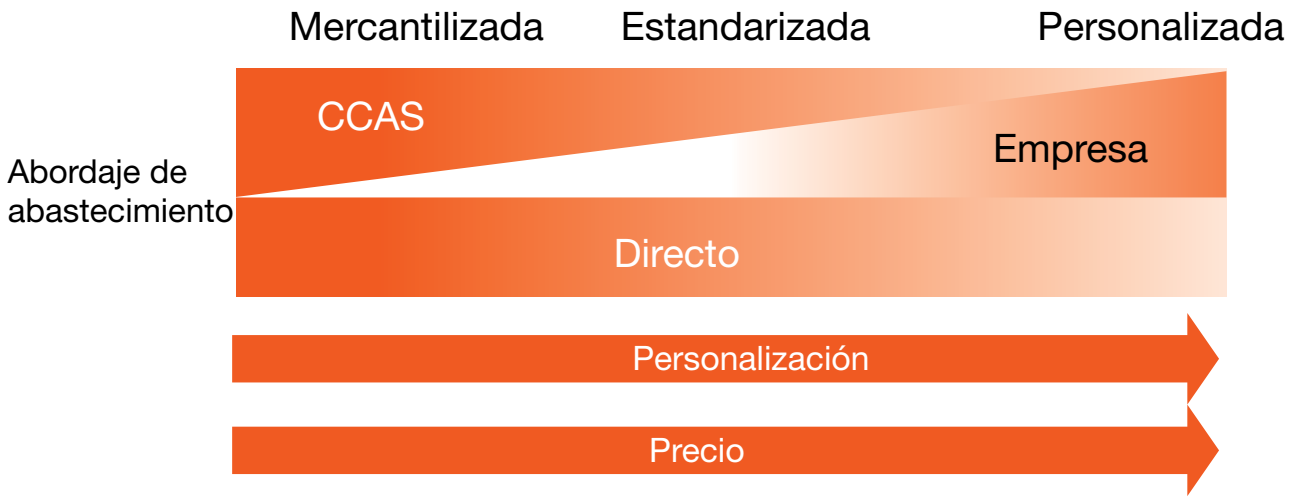
Muchas organizaciones que incorporaron y pusieron sus procesos existentes de autenticación basados en el conocimiento en estas plataformas ahora están comenzando a buscar enfoques de seguridad más modernos, como la biometría de voz. Estos son ahora significativamente más accesibles como resultado de las integraciones estandarizadas en estas plataformas y el aumento de la disponibilidad de servicios de biometría de voz basados en la nube.

Estratificación del mercado

Vemos una estratificación emergente del mercado de la biometría de voz, particularmente en lo que se refiere a los centros de contacto. En el extremo altamente personalizado del mercado se encuentran los principales proveedores de plataformas Nuance y Pindrop, que se centran en la autenticación y la prevención de fraudes. Estas soluciones son altamente personalizables, están respaldadas por amplios equipos de servicios profesionales y se pueden poner a trabajar con cualquier plataforma de telefonía subyacente.

Muy relacionadas con estas son las soluciones integradas de Verint y NICE. Cuando los clientes ya utilizan parte de sus respectivas suites, los gastos generales de implementación significativamente reducidos las convierten en una primera consideración lógica. Si bien aún no se han puesto en servicio de forma tan generalizada, estas soluciones son personalizables de manera similar, y tienen la ventaja significativa de un menor costo y complejidad de implementación (después de la implementación inicial de la suite). Esperamos ver un crecimiento sustancial de estos actores a medida que su extensa base instalada aprovecha la oportunidad de mejorar la autenticación y la prevención de fraudes.

Figura 3 - Estratificación del mercado de biometría de voz



En el extremo del mercado de materias primas, Amazon y Google han definido un nivel de precio muy bajo de 1-2c por autenticación, pero con oportunidades mínimas para la personalización, hasta ahora desconocido el rendimiento y restringida la disponibilidad a sus propias plataformas o socios. Queda por ver para qué verticales y casos de uso estas soluciones serán lo suficientemente buenas, pero esperamos que la disponibilidad de estos servicios despierte el interés de las empresas, incluso si posteriormente eligen otras opciones para su implementación. Si bien Amazon y Google pueden haber construido sus propias tecnologías, la mayoría de los proveedores de centros de contacto en la nube no pueden permitirse ese lujo. Sin embargo, para seguir siendo competitivos, son cada vez más de etiqueta blanca u ofrecen una estrecha integración con otros proveedores especializados que figuran en este Intelliview.

Entre estos dos polos, vemos la mayoría de los proveedores de biometría de voz con ofertas más estandarizadas. Sin enormes equipos de servicios profesionales, generalmente se centran en integrarse con un puñado de plataformas de telefonía (como la solución EVA de Auraya para Amazon Connect, la asociación de ValidSoft con Five9, Talkdesk [de etiqueta blanca] y Vonage, y VBG con Aspect), lo que reduce la complejidad de la implementación y les permite centrarse en el núcleo de la solución.

Esperamos que esta sección del mercado presente la máxima actividad en los próximos años a medida que la biometría de voz se vuelve deseable y accesible para una gama mucho más amplia de organizaciones. Los proveedores que se centran en esta sección deben enfocarse en el volumen de implementaciones, no en su escala individual, y asegurarse de que sus clientes logren los resultados empresariales y técnicos que desean. Es revelador observar que tanto Nuance como Pindrop están mejorando o complementando sus soluciones para satisfacer a este mercado.

Acceso y disponibilidad: "Hacer clic para comenzar"

El aprendizaje automático subyacente y el procesamiento de señales de biometría de voz pueden requerir doctorados y años de experiencia para comprenderlos, pero los mecanismos centrales de integración e implementación son relativamente simples. La mayoría de los desarrolladores pueden entender los conceptos básicos en menos de una hora. Es prometedor; que algunos proveedores estén haciendo que sus soluciones sean más fáciles para comenzar a usarlas. Esperamos que esto reduzca la incertidumbre y la percepción de complejidad en torno a estas soluciones que inevitablemente han impedido que muchas organizaciones progresen.

Amazon pone su servicio VoiceID para Amazon Connect a disposición de cualquier persona que tenga una tarjeta de crédito para probar, y cada vez es más fácil para las organizaciones enfocadas en desarrolladores comenzar con la biometría de voz. La solución EVA de Auraya, también para Amazon Connect, está disponible en el mercado de AWS con plantillas CloudFormation que soportan toda la infraestructura necesaria para una implementación de producción, así como un precio claro y transparente. El programa copiloto de VoiceIT proporciona acceso rápido a un entorno de espacio aislado junto con su extenso código de ejemplo en GitHub y referencias de API de fácil acceso. La oferta de VBG centrada en el desarrollador ofrece pruebas gratuitas de 60-90 días y opciones de pago por uso desde su sitio web. Phonexia proporciona a los desarrolladores un espacio aislado, y Veridas publica todas sus API en su sitio web. Nuance también puede proporcionar su plataforma Gatekeeper en la nube previa solicitud, y los espacios aislados basados en la nube de ValidSoft están disponibles a petición, ya sea directamente o preintegrados con sus socios.

Integración de análisis e inteligencia en plataformas

Las soluciones para los encuestados de nuestra plataforma han madurado durante el último año y se han vuelto cada vez más completas, integradas y fáciles de implementar.

Análisis de voz

El análisis de voz es ahora casi universal como un componente opcional de estas plataformas con diversos grados de integración. Esta tecnología se puede utilizar para identificar a los autores de llamadas que usan patrones de palabras indicativos de scripts fraudulentos, tratando de diseñar socialmente a los agentes, o a agentes que no cumplen las normas. Con productos dedicados de análisis de voz en su cartera, las implementaciones de NICE y Verint son probablemente las más versátiles. Aun así, la huella de conversación (Conversation Print) centrada en la seguridad de Nuance es posiblemente la más estrechamente integrada con la detección de fraude, al tener un éxito significativo con problemas desafiantes como el abuso de reembolsos. Esperamos ver esto como una parte cada vez más importante de las soluciones holísticas de IAuth en el futuro.

Análisis infundido por IA para la detección de fraude

A medida que aumenta la gama de puntos de datos disponibles para las plataformas, las permutaciones y combinaciones de resultados de diferentes métodos son cada vez más difíciles de planificar. Pindrop siempre ha producido una única puntuación basada en el riesgo a partir de sus numerosos métodos de detección de fraude. Ahora, Nuance está utilizando la IA en su motor de riesgos para optimizar los resultados empresariales con base en todos los métodos disponibles de autenticación y detección de fraude. Aún no estamos seguros de si todos los usuarios finales se sentirán cómodos con este nivel de abstracción. Sin embargo, para la mayoría, esta tendencia simplifica radicalmente la planificación y la implementación de estas tecnologías.

Agente de confianza

La COVID-19 aceleró muchas transformaciones, incluidas las operaciones remotas, distribuidas y de trabajo desde casa. Ello también ha aumentado los riesgos potenciales asociados al agente del centro de contacto remoto. Varios proveedores, incluidos ValidSoft, Nuance, Verint y VBG reconocieron esta necesidad y se apresuraron a llevar soluciones personalizadas al mercado que autentican continuamente a los agentes remotos para evitar la transferencia a proxies no autorizados que actúan en nombre del agente genuino. A medida que los reguladores se pongan al día con estos cambios en las prácticas de trabajo, esperamos que la demanda de estas soluciones aumente significativamente.

Inteligencia de red

Todos los encuestados de la plataforma dieron más importancia a las soluciones de inteligencia de red este año, reconociendo que no todas las personas que llaman probablemente estén dentro del alcance de tecnologías como la biometría de voz. La adquisición de Next Caller por parte de Pindrop, sumada a sus capacidades existentes, fue quizá el movimiento más audaz, pero el enfoque de colaboración de Nuance también cobró fuerza, y Verint está incorporando la capacidad a su solución de Fraude Adaptativo. Vemos un valor significativo en este tipo de soluciones no solo como parte de una plataforma, sino como soluciones por derecho propio (consulte a continuación) para verticales de menor riesgo y casos de uso. Como resultado, esperamos que el uso de estos datos se convierta rápidamente en un requisito básico para una solución de plataforma, ya sea a través de asociaciones o soluciones internas.

"UNA VEZ QUE SE IMPLEMENTÓ LA DETECCIÓN DE SUPLANTACIÓN DE ANI, LA ACTIVIDAD DE FRAUDE DISMINUYÓ SIGNIFICATIVAMENTE Y SE HA MANTENIDO ESTABLE DURANTE MÁS DE 4 AÑOS"

–Administrador de productos, Global Financial Holding Company

Integración

Como proveedor de CCaaS por derecho propio, nos alegramos de que NICE finalmente llevara su solución de autenticación en tiempo real a CXone, proporcionando la solución de marca propia más completa de cualquier proveedor de CCaaS. Al mismo tiempo, Nuance y Pindrop aumentaron la profundidad y sofisticación de sus integraciones con otras plataformas en la nube como Amazon Connect y Five9. También mejoraron la facilidad de integración con plataformas locales más tradicionales. Es cada vez más fácil comenzar a usar estas plataformas, cada encuestado ahora tiene alguna forma de oferta de SaaS para evaluar su efectividad con datos del mundo real sin meses (y a veces años) de costoso esfuerzo de implementación. Muchos de los clientes tradicionales de nuestros encuestados están evaluando o cambiando a soluciones CCaaS que requieren que los proveedores desarrollen nuevas integraciones y mejoren las existentes. Esperamos una mayor disponibilidad y un menor costo de propiedad para que estas soluciones sean relevantes para un mercado más amplio que el actual.

Presentación de dos nuevas categorías de IAuth

El mercado de IAuth sigue evolucionando, y nos complace incluir este año dos nuevas categorías junto con la tecnología de biometría de voz y las plataformas:

Autenticación de red y detección de fraude

La autenticación de red y la detección de fraude utilizan la señalización y otros datos de inteligencia de red para aumentar la confianza de que el número presentado es el que dice ser. Permiten la autenticación basada en la posesión y la detección de anomalías para identificar llamadas potencialmente fraudulentas. Smartnumbers, Neustar, Prove y Next Caller protegen más de 5000 millones de interacciones con los clientes, y tecnología similar también es aprovechada por soluciones de plataforma de Nuance, Pindrop y Verint. Estas soluciones brindan a muchas organizaciones un primer paso fácil hacia la IAuth sin las integraciones más complejas y los requisitos de inscripción de la biometría de voz.

Las soluciones de autenticación de red aumentan la confianza de que la ANI asociada a una llamada no se ha falsificado o cambiado recientemente a un nuevo dispositivo para que, sujeto a coincidencias en los registros de las empresas, el número presentado se utilice para autenticar a los autores de llamadas para transacciones de menor riesgo. Respecto a aquellas llamadas que no coinciden o presentan algunas anomalías, estas soluciones utilizan su comprensión de los patrones de enrutamiento fraudulentos típicos y conocidos a fin de evaluar el riesgo de que la llamada sea fraudulenta y tratarla en consecuencia. Next Caller, por ejemplo, ha mapeado hasta ahora más de 3 millones de rutas únicas. Las características clave que evaluamos incluyeron:

- **Detección de suplantación de identidad**: la capacidad de detectar si la ANI o CLI presentada es genuina o ha sido suplantada.
- **Evaluación de riesgos de enrutamiento de llamadas**: la capacidad de identificar las rutas de red que tienen más probabilidades de estar asociadas a una actividad fraudulenta.
- **Lista de seguimiento y detección de velocidad**: la capacidad de detectar dispositivos de origen fraudulento conocidos y llamadas de alta frecuencia sospechosas de otros dispositivos.
- **Detección de cambio de dispositivo/intercambio de SIM**: la capacidad de detectar si el dispositivo de origen de un número presentado ha cambiado recientemente o se ha transferido a otro dispositivo o red.
- **Administración de casos**: herramientas para permitir que los analistas de fraude investiguen llamadas sospechosas, con inclusión de comentarios para mejorar el rendimiento futuro de la solución
- **Integración**: algunas soluciones están profundamente integradas con ciertos operadores o provienen de proveedores con acceso privilegiado a la red, lo que, si bien proporciona beneficios significativos, puede limitar su aplicación en otros contextos.

"EL OBJETIVO DEL PROYECTO ERA CLARO: REDUCIR LA FRICCIÓN DE LOS CLIENTES AL TIEMPO QUE MANTENER LA INTEGRIDAD DE NUESTRA PREVENCIÓN DE FRAUDES. ... LOS RESULTADOS (DEL ANÁLISIS DEL COMPORTAMIENTO) SUPERARON LAS EXPECTATIVAS, Y EL RENDIMIENTO SIGUE SIENDO ESTABLE".

—Director de Préstamos, EE.UU. Regional Lending Services Firm

---

Biometría de comportamiento

Los proveedores de biométrica de comportamiento respaldan técnicas para que las empresas detecten impostores o autentiquen a clientes genuinos en función de la forma única en que las personas interactúan con sus dispositivos, incluida la forma en que sostienen su teléfono inteligente o si usan dos pulgares o su dedo índice para escribir. A medida que una creciente cantidad de comercio humano se lleva a cabo en línea o a través de dispositivos móviles, y a medida que el "conocimiento cero", el anonimato y el pseudonimato se afianzan, el análisis basado en el comportamiento asigna puntuaciones de riesgo a individuos o dispositivos estrictamente en función de sus acciones, comparándolas con los comportamientos conocidos o los de impostores conocidos.

Tres empresas —BehavioSec, BioCatch y Threatmark— respondieron a nuestras solicitudes de información. Cada una se distingue por adoptar un enfoque único para detectar rasgos anómalos que indican un mayor riesgo de que un individuo se comporte como un impostor, en lugar de un cliente o un cliente potencial auténtico. Prevemos que sus tecnologías adquirirán mayor importancia a medida que el uso de IAuth se expanda a las empresas que quieren detectar posibles fraudes iniciados por personas que contactan con una empresa con poca frecuencia o por primera vez.

Mapas de Intelliview

Para ayudar a los responsables de la toma de decisiones a evaluar a los proveedores de soluciones de la competencia, Opus Research representa su posicionamiento en una serie de "Mapas de Intelliview". Con respecto a las figuras 4, 5, 6 y 7, hemos clasificado a los proveedores de soluciones según su posición relativa en el mercado y su éxito. El tamaño de las figuras ovales de Intelliview refleja dos factores muy importantes:

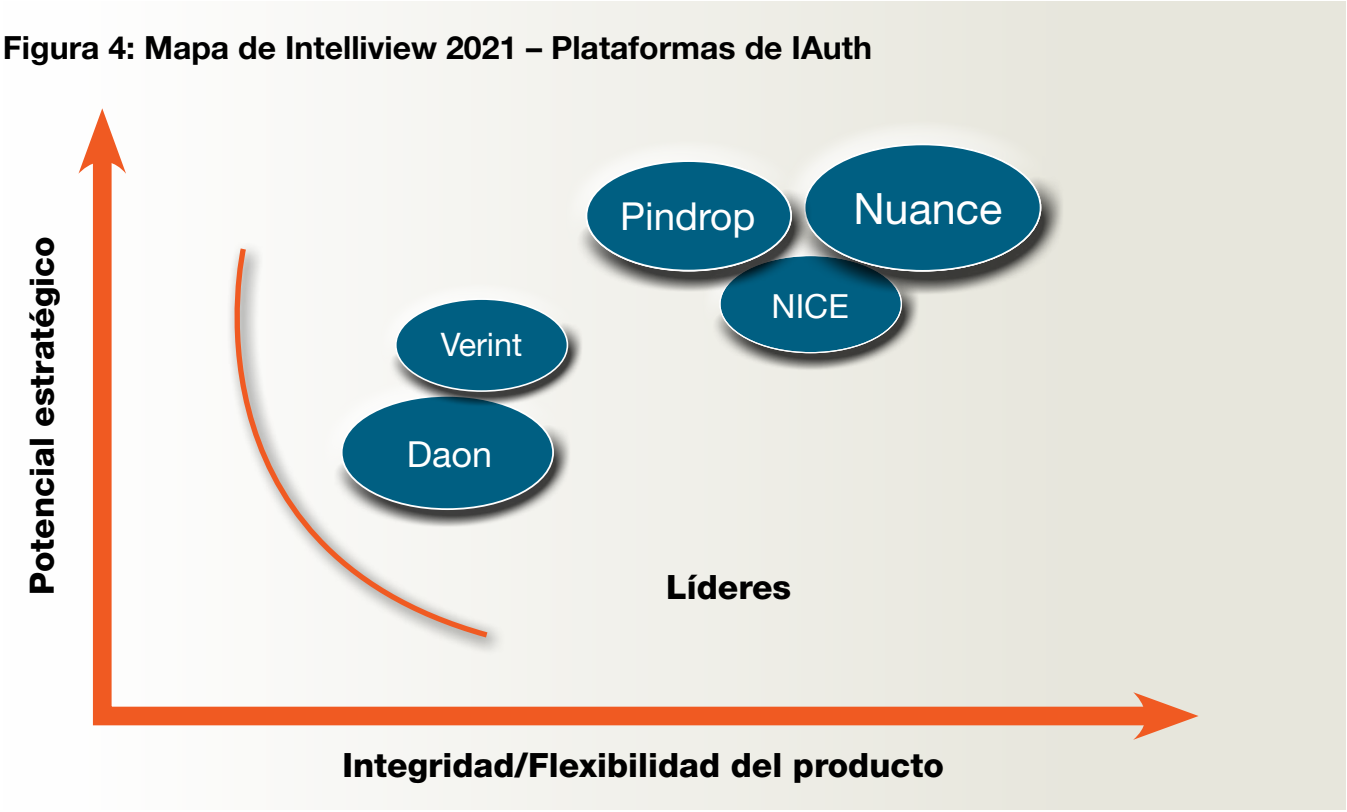
- **Completitud/flexibilidad del producto**: captura cómo las capacidades actuales del producto cumplen con los requisitos reales del cliente, como lo demuestran las implementaciones a las que se hace referencia. Incluye una evaluación de la flexibilidad para adaptarse a las necesidades específicas como lo demuestran los clientes de referencia. Los proveedores de plataformas reciben la evaluación más alta cuando sus capacidades son "amplias". Sus servicios y características generalmente cubren todas las columnas de la pila de soluciones: Autenticación, prevención de fraudes, orquestación y aplicaciones. Los proveedores de tecnología básica reciben las evaluaciones más altas cuando sus capacidades son "profundas". Ello incluye la validación externa del rendimiento, las estrategias para mitigar vulnerabilidades comunes, la disponibilidad y calidad de la documentación de API y los enfoques de poco esfuerzo para ajustar y calibrar la tecnología básica en una amplia variedad de casos de uso de autenticación y detección de fraude.

- **Potencial estratégico**: captura cómo la visión y la hoja de ruta apelan a los requisitos tecnológicos actuales y en evolución en centros de contacto y más allá. Incluye una evaluación del ecosistema de socios e integradores de salida al mercado de cada empresa. Los proveedores de plataformas reciben las evaluaciones más altas cuando pueden demostrar una amplia compatibilidad con una amplia gama de factores y plataformas de telefonía. Los proveedores de tecnología básica reciben las evaluaciones más altas cuando pueden demostrar una inversión continua en mejoras de rendimiento y evolución de productos.

El tamaño de los óvalos representa el impacto en el mercado de cada proveedor en función de la información de clientes, interacciones aseguradas o usuarios inscritos proporcionada por la empresa o disponible públicamente. Se modifica mediante una evaluación de la solidez financiera actual (ingresos, rentabilidad, respaldo financiero, longevidad y tamaño de la base de clientes).

Plataformas

Figura 4: Mapa de Intelliview 2021 – Plataformas de IAuth



Líderes (en orden alfabético)

Cada encuestado de esta categoría gana su lugar en el segmento de líderes al distinguirse en una o más áreas de nuestro análisis. En la práctica, la solución adecuada para cualquier empresa depende de factores que incluyen el valor en riesgo, la escala y la complejidad de la organización y las inversiones en tecnología existentes. Sin embargo, todos los encuestados de este año merecen consideración.

Daon

Daon ha logrado su papel de liderazgo al centrarse en su solución IdentityX. Admite una amplia gama de mecanismos biométricos y alternativos de autenticación para la incorporación digital y la autenticación continua. Permite a las organizaciones combinar el mecanismo más apropiado respecto a los casos de uso en el centro de contacto, en persona y móvil que abarcan los Servicios Financieros, Viajes y Hospitalidad, el Sector Público. Adoptando un enfoque al que se refiere como "Continuidad de identidad", Daon respalda una visión para aplicar el factor biométrico o de autenticación apropiado que comienza con la incorporación y luego abarca la autenticación en el dispositivo o a través de los recursos del centro de contacto.

NICE

La autenticación en tiempo real (RTA) de NICE utiliza la profunda integración de su plataforma con el centro de contacto para proporcionar a sus clientes existentes una solución atractiva de autenticación y prevención de fraudes. Al acceder a las grabaciones históricas, RTA puede preinscribir a las personas que llaman e identificar de forma proactiva a los defraudadores a partir de la exploración de cientos de miles de llamadas a fin de ofrecer valor

empresarial el primer día de la implementación con un esfuerzo adicional mínimo. Los resultados de autenticación y prevención de fraudes se muestran utilizando sus herramientas de escritorio y back-office de agente existentes, lo que requiere poca capacitación o formación adicional. La solución complementaria de NICE "Prevención de fraudes habilitada" basada en su análisis de voz Nexidia puede identificar comportamientos anómalos y fraudulentos. Estas capacidades también están disponibles de inmediato para los clientes de la plataforma del centro de contacto de Nice CXone.

Nuance

Nuance sigue dominando el mercado con el mayor número de implementaciones y autenticaciones anuales. Su solución Gatekeeper basada en la nube está ganando nuevos clientes empresariales y del mercado medio y migraciones desde implementaciones locales existentes. La solución en sí sigue evolucionando, con nuevas características que se ponen a disposición regularmente. El motor biométrico de voz Lightning de Nuance continúa elevando el límite de rendimiento al inspirar una gran confianza en las expresiones cortas que se encuentran habitualmente en IVR (otra gran parte del negocio de Nuance). Ahora se centran en poder inscribir a los usuarios con expresiones igualmente cortas que reducen los requisitos de registro del agente. Respecto a la prevención de fraudes, Nuance continúa invirtiendo en herramientas para mejorar la experiencia del analista y compartir conocimientos y experiencia a través de su centro de excelencia Fraud Nexus. En el horizonte, el motor de riesgo de IA de Nuance tiene como objetivo simplificar la gestión de umbrales y combinaciones cuando se utilizan múltiples autenticaciones y factores de detección de fraude mediante el enfoque en los resultados empresariales.

Pindrop

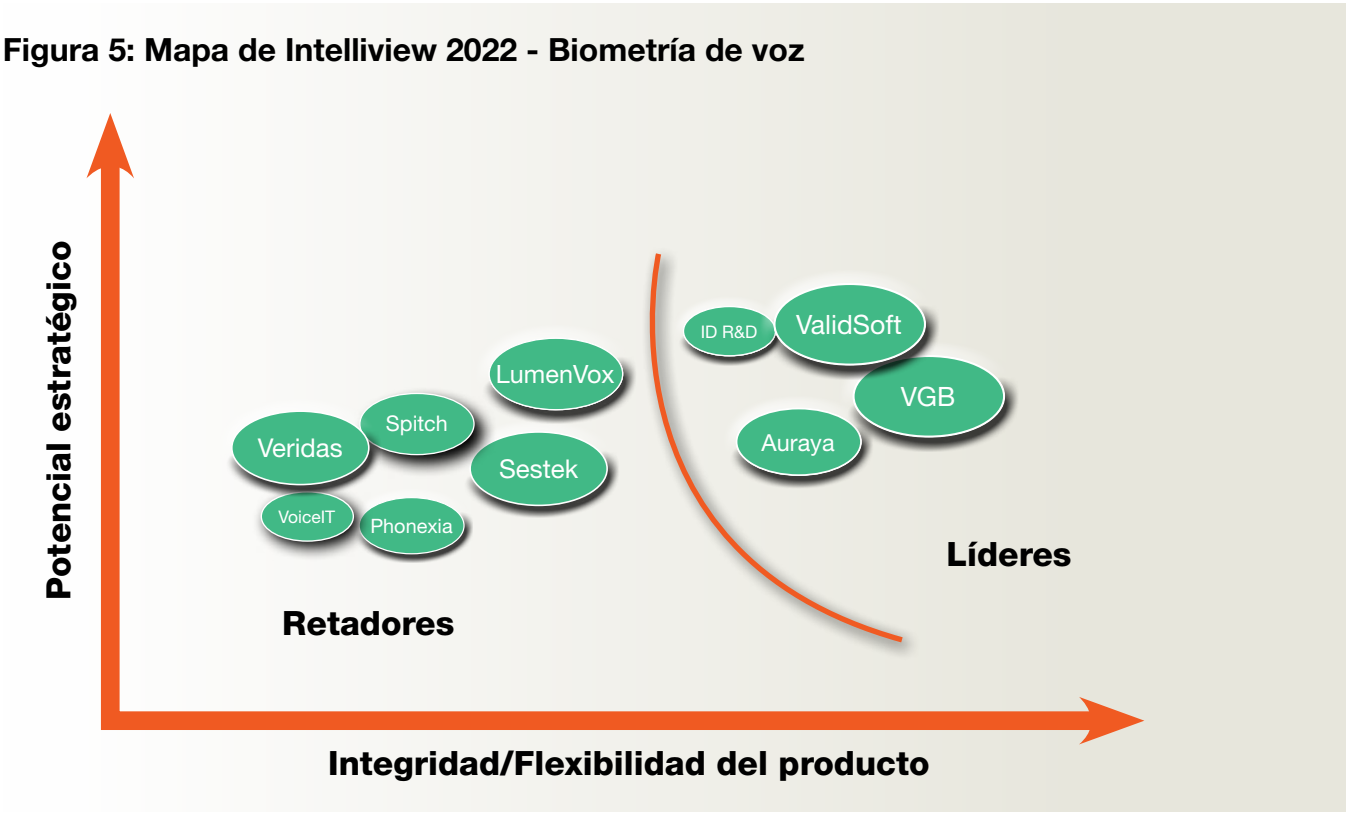
El enfoque histórico de Pindrop en la prevención de fraudes continúa con la mejor experiencia de analista de su clase y nuevas herramientas para predecir qué cuentas están más en riesgo antes de cualquier pérdida. Su tecnología de impresión telefónica y los datos del consorcio ahora cubren casi 5000 millones de llamadas y 2 millones de eventos de fraude. Su solución de autenticación basada en biometría de voz de pasaporte se ha actualizado con la versión 3 de su algoritmo Deep Voice, prometiendo resultados de autenticación aún más rápidos y precisos. La solución basada en la nube está disponible en Europa por primera vez. La adquisición, por parte de Pindrop, de Next Caller (que también aparece por separado en Autenticación de red y Detección de fraude) fortalece sus servicios de validación de identificadores de llamadas y los datos del consorcio existentes. También hace que las soluciones de Pindrop sean relevantes para una proporción mucho más amplia del mercado.

Verint

La amplia cartera de Verint incluye dos soluciones. El fraude adaptativo es una solución integral basada en los conocimientos obtenidos al operar uno de los IVR alojados más grandes de América del Norte y respaldado por un equipo experimentado. Incluye capacidades de análisis de comportamiento e inteligencia de red para identificar llamadas fraudulentas junto con su lista de seguimiento de Sentry, que identifica cuentas en riesgo, permitiendo a los clientes lograr un autoservicio y enrutamiento de llamadas con base en el riesgo. La autenticación de identidad y la detección de fraude mediante biometría de voz están arraigadas en su tecnología de grabación de llamadas y están estrechamente integradas con sus aplicaciones de escritorio y back-office de agentes, lo que facilita mucho la implementación y es una consideración lógica para los clientes existentes. La tecnología de análisis de voz de Verint puede identificar de manera similar el comportamiento sospechoso y desencadenar respuestas apropiadas después de las llamadas.

Biometría de voz

Figura 5: Mapa de Intelliview 2022 - Biometría de voz



Líderes (en orden alfabético)

Nuestros líderes del mercado se distinguen por el claro vínculo entre su amplia experiencia en implementación, soluciones maduras y un profundo enfoque en la biometría de voz o la autenticación.

Auraya

La amplia experiencia de implementación de Auraya con su suite ArmorVox brilla en su solución EVA. EVA envuelve la interfaz de usuario esencial y la lógica empresarial alrededor del motor ArmorVox para acelerar la implementación. Esta solución incorpora la autenticación y la detección de fraude en una solución empaquetada que puede estar lista y en funcionamiento en unos pocos clics con precios transparentes cuando se implementa en AWS. La capacidad de EVA para cruzar de manera eficiente millones de llamadas junto con sus modelos de fondo por altavoz son características destacadas.

IDR&D

IDR&D se centra principalmente en la aplicación de la biometría facial y de voz a los casos de uso de dispositivos móviles. Su enfoque en la biometría de voz de alto rendimiento, particularmente en la derrota de los ataques de presentación junto con la creciente tracción en sus mercados objetivo, les confiere un espacio en la categoría de líder. Deben incluirse en cualquier evaluación de la biometría de voz para casos de uso novedosos.

ValidSoft

ValidSoft se destaca por su énfasis en la privacidad por diseño y el cumplimiento de los estrictos estándares

europeos de sellos de privacidad. Las importantes ganancias de Fortune 50 han reconocido recientemente la vasta experiencia técnica de ValidSoft. Se ganan su espacio en la categoría de Líderes gracias a estas victorias y a sus asociaciones demostrablemente sólidas con Five9, Talkdesk, Vonage y otros, lo que impulsa una mayor adopción. La tecnología básica de ValidSoft se puede empaquetar en todos los modos de implementación imaginables, incluyendo su propia solución alojada y aplicaciones integradas/en el dispositivo.

Voice Biometrics Group (VBG)

VBG es la segunda en número de implementaciones de biometría de voz pura después de Nuance. Con un enfoque exclusivo en este mercado, su solución continúa evolucionando con el mismo énfasis en el rendimiento del motor central y la experiencia de usuario/resultados empresariales. Nos ha impresionado en particular la interfaz de usuario administrativa, que refleja claramente las lecciones que tanto ha costado aprender de las experiencias de implementación. Tienen una base de clientes notablemente diversa y cada vez más global, lo que garantiza que la mayoría de los casos de uso o requisitos imaginables se puedan cumplir con una amplia gama de modelos de implementación (incluida la nube alojada) disponibles. Un cliente informó: "Su capacidad de respuesta y su disposición a ser flexibles con las tecnologías de vanguardia no tienen precedentes".

Retadores (en orden alfabético)

Por supuesto, hay muchos más proveedores de tecnología de los que podríamos mostrar aquí. Aun así, cada encuestado en esta categoría tiene atributos únicos que lo hacen excepcionalmente adecuado para algunos casos de uso y mercados. Dada su trayectoria, esperamos que varios sean futuros líderes, de ahí el apodo de "los que vigilar".

LumenVox

El pedigrí de LumenVox como uno de los proveedores de reconocimiento de voz preeminentes proporciona una base sólida para su solución de biometría de voz. Como resultado de su fusión con VoiceTrust en 2018, su solución dependiente e independiente de texto es utilizada por varios integradores de sistemas y proveedores de soluciones. Su solución de restablecimiento de contraseña empaquetada resuelve un problema sorprendentemente grande para las grandes empresas y sigue siendo popular. Un socio informó: "Existe un respeto y apoyo mutuo por la oferta de los demás, y seguimos colaborando en nuevas oportunidades en nuestro mercado".

Phonexia

La larga experiencia de Phonexia en biometría de voz y reconocimiento de voz para casos de uso de seguridad pública proporciona una base sólida para su oferta comercial. Proporcionando solo soluciones independientes del texto, su espacio aislado se puede poner a prueba en cuestión de horas. A juzgar por el número de evaluaciones en curso y la capacidad de soluciones, no pasará mucho tiempo antes de que ganen negocios significativos en sus mercados objetivo. Su motor moderno está optimizado para la autenticación de expresiones cortas, y estamos particularmente impresionados por los resultados que han obtenido dado su poco tiempo en este mercado.

Sestek

Sestek es el proveedor líder de soluciones de voz de todo tipo en Turquía y Oriente Medio. Dado que Turquía tiene más huellas de voz en uso per cápita que cualquier otro país a nivel mundial, no es sorprendente que sus soluciones sean particularmente maduras y capaces de conseguir clientes contra proveedores tradicionales consolidados. Su base de clientes incluye los principales servicios financieros y operadores de telecomunicaciones de su mercado objetivo. Su solución cubre casos de uso de autenticación y prevención de fraudes y se puede implementar en aplicaciones móviles o centros de contacto junto con su plataforma de IA conversacional.

Spitch

Con sede en Zúrich, Spitch se centra en una variedad de soluciones de voz, incluidos asistentes virtuales y análisis de voz, particularmente para idiomas distintos al inglés. Su éxito con la biometría de voz en el mercado suizo (donde la mayoría de las organizaciones necesitan admitir tres idiomas diferentes y cumplir con algunas de las leyes de privacidad más estrictas), notoriamente exigente con los bancos y otros, es un testimonio de su perseverancia y capacidad técnica. Su solución independiente de texto incluye la detección de fraudes, pero también se puede integrar con su producto de análisis de voz para detectar nuevos defraudadores mediante el uso de lenguaje de scripts o anómalo.

Veridas

Una nueva participante en el Intelliview de este año, Veridas se centra completamente en el reconocimiento de documentos, la biometría de voz y facial para los casos de uso de autenticación, prevención de fraudes y prueba de identidad. Con sede en España, tienen considerable aceptación en los mercados de habla hispana y están obteniendo cada vez más éxito en otros lugares, incluido un logro de gran repercusión en Deutsche Telekom por su solución de biometría de voz. Sus API y datos de rendimiento están disponibles para cualquier persona en su sitio web centrado en el desarrollador.

VoiceIT

VoiceIT fue el proveedor original de biometría de voz y facial de SaaS. Si bien se mantienen fieles a sus raíces centradas en el desarrollador con API disponibles públicamente y ejemplos de código, ahora están agregando autenticación independiente de texto a su solución. Su programa de incorporación "Copiloto" proporciona un proceso paso a paso que garantiza que los desarrolladores obtengan el soporte que necesitan y puedan navegar rápidamente por los desafíos de privacidad y calibración de la tecnología.

Proveedores de la nube

Sin aparecer en un gráfico de Opus Research Intelliview anterior, pero incluidos a efectos de exhaustividad, los gigantes de la computación en la nube también han entrado en el mercado de la biometría de voz con soluciones disruptivas y mercantilizadas.

Amazon

El servicio VoiceID de Amazon entró en beta en enero de 2021 y estuvo disponible en general en septiembre de 2021, agregando la detección de fraude basada en listas de seguimiento al caso de uso de autenticación existente. La solución independiente de texto solo funciona con Amazon Connect. Aun así, para los usuarios de la plataforma, la integración es impresionantemente fácil de implementar; y a 2.5C por transacción (inscripción y autenticaciones), el precio resulta muy competitivo. Después de un rápido proceso de incorporación, los componentes de VoiceID se pueden soltar en los flujos de llamadas existentes, y los agentes pueden completar todas las acciones de inscripción y autenticación requeridas utilizando la interfaz estándar. Todavía no existe un mecanismo para calibrar o evaluar el rendimiento del modelo biométrico subyacente, por lo que sus aplicaciones en el mundo real pueden limitarse a casos de uso de menor riesgo.

Google

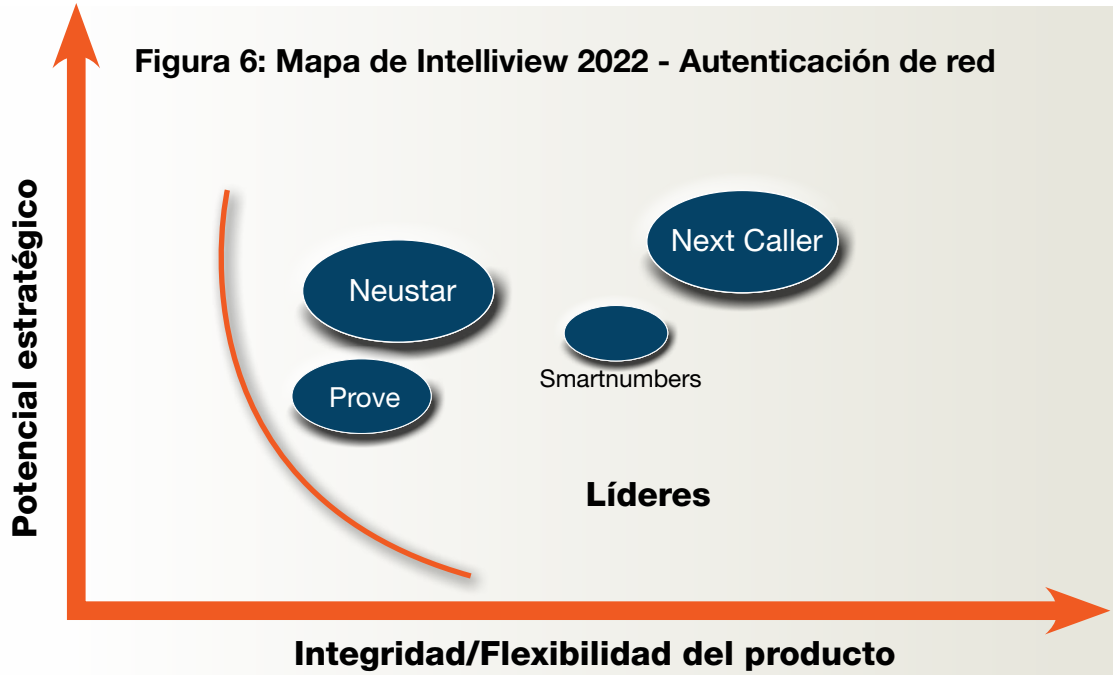
Google anunció ID del hablante como parte de su propuesta de Inteligencia Artificial de Centros de Contacto (CCAI) en octubre de 2021. La solución solo está disponible a través de socios (incluidos Genesys y Avaya), y no hay documentación disponible públicamente, por lo que es difícil sacar demasiadas conclusiones. Lo que está claro es que es probable que la implementación inicial esté más cerca del texto solicitado que de texto verdadero independiente y limitado a la solución de lenguaje natural Dialogflow de Google. Sin embargo, el anuncio de Google valida aún más cuán esencial es la autenticación basada en voz para este tipo de soluciones y socava la de Amazon a 1 c por autenticación.

Microsoft

El servicio de reconocimiento del hablante de Microsoft forma parte de Azure Cognitive Services. Si bien la API ha estado disponible en vista previa durante varios años, recientemente agregó funciones independientes de texto y se puso a disposición general en noviembre de 2021. La API básica se proporciona con ejemplos de código en todos los lenguajes de programación concebibles. Admite casos de uso tanto independientes como dependientes de texto para la identificación (hasta 50 candidatos, por lo que también podrían usarse para listas de seguimiento de fraude limitadas) y la autenticación. Entre 0,5 C y 0,3 C por transacción, dependiendo del volumen, su precio es excepcionalmente competitivo. Al igual que todos los grandes servicios de nube, simplemente proporciona una puntuación numérica que depende de los usuarios finales para determinar si es suficientemente confiable para su caso de uso. Microsoft también insiste en que los usuarios inscritos pronuncien una frase de activación específica al comienzo de su inscripción. Si bien se enfrenta de manera efectiva al desafío de la privacidad, es probable que sea difícil implementar en los escenarios del centro de llamadas.

Autenticación de red y prevención de fraudes

Figura 6: Mapa de Intelliview 2022 - Autenticación de red



Líderes (enumerados alfabéticamente)

El mercado de autenticación de redes y prevención de fraudes incluye muchas más empresas que nuestros encuestados. Aun así, todos nuestros encuestados se ganan su lugar en nuestra categoría de líderes del mercado al demostrar fuerza de mercado, capacidad técnica y promesa estratégica.

Neustar

Las soluciones de Neustar combinan su adquisición de TRUSTID en 2019 con su condición de proveedor de la mayor parte de la infraestructura de identificación de llamadas de los EE. UU. Forman parte del negocio que está adquiriendo TransUnion. La autenticación entrante de Neustar incluye su tecnología patentada de autenticación previa a la respuesta que permite que las llamadas de alto riesgo sean tratadas de manera diferente incluso antes de conectarse con la infraestructura del usuario final. Su condición de operador privilegiado les permite confirmar que el dispositivo reclamado está realmente en uso.

Cuando no es un dispositivo único, utilizan su experiencia de miles de millones de llamadas para evaluar el riesgo de suplantación de identidad. Se puede integrar aún más con su solución de base de datos OneID para identificar al propietario de ANI desconocidas, aumentando la identificación y las tasas de autenticación posteriores.

Next Caller

Adquirida por Pindrop en marzo de 2021, Next Caller complementa la plataforma más amplia de Pindrop y continúa operando como una empresa separada, por lo que está incluida en esta categoría por derecho propio. La solución VeriCall de Next Caller cubre miles de millones de llamadas al año y ha catalogado millones de rutas de operador únicas. VeriCall proporciona una puntuación de confianza con códigos de motivo que reflejan una amplia gama de factores de riesgo basados en datos de señalización a través de una llamada API rápida que permite a los usuarios finales tomar decisiones de enrutamiento y tratamiento adecuadas dependiendo del resultado y confiando en el identificador de llamadas para la autenticación cuando corresponda. Un cliente con el que hablamos describió su relación con Next Caller como "muy positiva" y había visto mejoras en las tasas de autenticación año tras año sin aumento en el fraude. La solución está disponible en mercados fuera de los EE. UU.

Prove

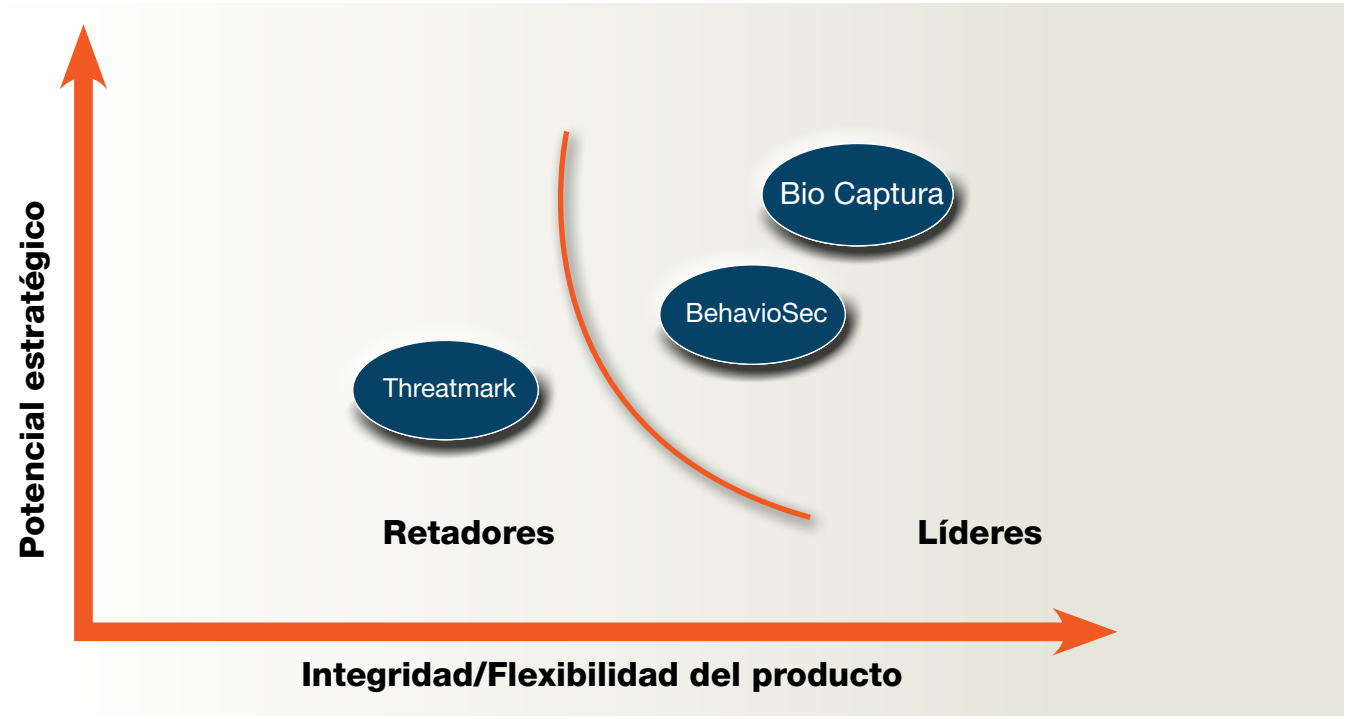
Prove (anteriormente Payfone) cambió de nombre a principios de 2021 y, con inclusión de la adquisición anterior de Early Warning Services, ahora sirve a 9 de los 10 principales bancos en los EE. UU., cubriendo miles de millones de llamadas cada año. Prove tiene asociaciones con portadoras y operadores de redes móviles en los EE. UU., Canadá y el Reino Unido, lo que le permite aprovechar la autenticación del dispositivo de los propios operadores para verificar la posesión e identificar los intercambios de SIM. La solución de Prove puede utilizarse para la prueba de identidad (confirmando al propietario de un teléfono para la incorporación), la autenticación y la detección de fraudes. Su oferta más amplia incluye análisis de comportamiento basados en dispositivos únicos que mantienen un conocimiento continuo de la posesión del dispositivo (incluso cuando no está en uso) desde su adquisición de UnifyID en junio de 2021 y autenticación de múltiples factores basada en push que proporciona una solución integral para organizaciones móviles.

Smartnumbers

Smartnumbers UK Heritage ha supuesto superar algunos desafíos difíciles en materia de regulación de la privacidad y, al mismo tiempo, ayudar a sus grandes clientes empresariales a mitigar los importantes volúmenes de fraude y reducir el esfuerzo de autenticación de los clientes. Son el proveedor predeterminado de los bancos más grandes del Reino Unido. Al tiempo que aprovechan su acceso privilegiado a la red en el Reino Unido, su solución Protect también se puede implementar de forma independiente de los operadores, lo que permite una implementación rápida a nivel mundial. Su capacidad de administración de casos permitirá a los analistas gestionar el proceso de investigación de fraudes de manera eficiente, y sus modelos estándar de la industria contribuirán aún más a poner a los clientes en funcionamiento rápidamente. Operan exclusivamente a través de socios, especialmente BT y Nuance, lo que les da muchas promesas estratégicas para expandirse más allá de sus mercados tradicionales.

Biometría de comportamiento

Figura 7: Mapa de Intelliview 2022 - Biometría de Comportamiento



Líderes (listados en orden alfabético)

Cada participante en la categoría de Biometría de Comportamiento se califica en función de la integridad de su oferta principal, así como de su capacidad demostrada para integrarse con las iniciativas existentes de autenticación y prevención de fraudes de una empresa. Como tecnología emergente, la biometría de comportamiento aún no comprende una solución única y completa para los esfuerzos de autenticación o prevención de fraudes y siempre será parte de una solución más amplia que abarque la inscripción, devolviendo una puntuación de confianza cuando se le solicite autenticar a un individuo conocido y alertando a las empresas cuando ciertos rasgos de comportamiento indiquen que es muy probable que un individuo sea un impostor.

BehavioSec

Fundada en 2008 y considerada la pionera de la categoría de biometría de comportamiento, ha aumentado su conjunto de capacidades orgánicamente como respuesta a la demanda de mecanismos transparentes para mejorar los métodos de autenticación obsoletos y vulnerables, como las "contraseñas únicas" basadas en SMS y las preguntas basadas en el conocimiento, al tiempo que acelera su desaparición al proporcionar un reemplazo viable y sostenible. Sus tecnologías básicas utilizan la cadencia, las interacciones con la pantalla táctil y los movimientos del mouse/trackpad para evaluar si la entrada proviene del usuario esperado o de un defraudador. Las "señales" que detectan sus motores analíticos se utilizan luego como entradas en un motor de riesgo más amplio, una plataforma de identificación o herramientas de terceros. Cabe destacar que la detección que hace su solución del cambio de IP, el origen desde un nuevo país y la discrepancia de ubicaciones superpone o mejora soluciones de los proveedores de inteligencia de red y autenticación.

BioCatch

Alega un enfoque exclusivo en la biometría de comportamiento, centrándose principalmente en la detección de fraude. Sin autenticación. Se distinguen por un largo historial y un profundo enfoque en los flujos de trabajo de los "operadores de fraude". Supervisan la gama más amplia de indicadores físicos y cognitivos (reclamando 2000) y patentes (60). También se distinguen por su comprensión de los procesos que simplifican las tareas del personal de Fraudes. Por ejemplo, permite a los operadores de fraude definir y proponer nuevas normas a medida que surgen y define un período de 7 días para que sean provisionales y luego un mecanismo para que un "usuario con permiso relevante" lo apruebe.

Retador

Threatmark

Un encuestado que dificulta la distinción entre Inteligencia de Red y Biometría de Comportamiento. Su puntuación se basa en que la "Reputación del dispositivo" se construye en la "huella digital extensa del dispositivo". Sin embargo, también afirma realizar una cantidad significativa de perfiles de comportamiento y, de hecho, cree que "la forma más confiable y eficiente de detectar el intercambio de SIM es mediante perfiles de comportamiento" porque los defraudadores no pueden replicar la biometría de comportamiento del usuario legítimo. Con base en la supervisión constante en segundo plano, puede proporcionar puntuaciones de riesgo basadas en la supervisión en tiempo real de los comportamientos que se realizan en un servidor central de análisis, que aplica ML e "IA" para obtener una puntuación en tiempo real.

Soluciones inteligentes para la autenticación de poco esfuerzo y detección de fraude

Las empresas están empezando a lidiar con cambios permanentes en la forma en que sus empleados y clientes trabajan, compran y buscan asistencia. Grandes porcentajes de empleados, incluidos los agentes del centro de contacto, quieren seguir trabajando en casa... al menos una parte del tiempo. Los clientes continúan queriendo comprar o buscar asistencia en bancos o tiendas cercanas, aun cuando sus actividades en línea y basadas en teléfonos inteligentes crecen. Los profesionales de la seguridad se ven obligados a tratar cada nuevo contacto como un primer encuentro. Aprovechar al máximo la información disponible para determinar en quién confiar y lo que pueden lograr.

En 2022, la frase clave será "hacer más con menos". No haga preguntas sin sentido. No confíe en las contraseñas. No haga que los clientes hagan el trabajo. En cambio, trabaje en segundo plano utilizando características físicas y de comportamiento (biometría) y "metadatos" generados en el transcurso de la interacción para aumentar la confianza de que el usuario es quien dice ser. Las empresas y tecnologías que se examinan en el presente documento son perfectamente idóneas para ayudar a las empresas a elaborar estrategias para un comercio de conversación seguro y confiable.

Nuance

Sede: Burlington, MA.
Año de inicio de la empresa: 1992
Inversión/financiación: N/A
Ingresos: Ingresos de 2020: ~ USD 1.500 millones
Número de empleados: Aproximadamente 7.100 empleados en total.

CAPACIDADES

Tecnología: biometría de voz

Autenticación básica
El motor de biometría de voz de Nuance utiliza redes neuronales profundas de última generación para autenticar a una persona con tan solo 0,5 segundos de audio y lograr tasas de éxito de autenticación de hasta el 99%. El sistema autentica a los clientes legítimos y detecta a los defraudadores conocidos comparando el audio de voz de entrada con una colección de muestras de voz almacenadas ("huellas de voz") que se sabe que son auténticas o fraudulentas. Las huellas de voz pueden inscribirse con tan solo 5 segundos de audio. El motor de biometría de voz de Nuance está protegido contra la transformación de voz, texto a voz adaptativo y otras formas de suplantación de audio. Admite tanto la autenticación de voz independiente de texto (pasiva) como la dependiente de texto (activa), incluida la autenticación de voz independiente de texto en el IVR y en el centro de contacto. Y puede autenticar con precisión a una persona a través del ruido de fondo, enfermedades, máscaras faciales y otros factores que de alguna manera modulan el sonido de la voz de una persona.

Dependiente de texto: Una implementación de biometría de voz dependiente de texto le pide a una persona que repita una contraseña vocal específica que coincida con la frase que grabó cuando inscribió su huella de voz. El motor de biometría de voz de Nuance prácticamente elimina la necesidad de verificación dependiente de texto debido a su precisión extremadamente alta y bajos requisitos de audio para la verificación independiente de texto de corta duración.

Independiente de texto: Una implementación de biometría de voz independiente de texto funciona continuamente en segundo plano para verificar a una persona a partir de su voz natural cuando interactúa con un agente humano o virtual, como un IVR habilitado para voz. Las últimas mejoras de Nuance en nuestro motor de biometría de voz logran un rendimiento suficiente para permitir a las organizaciones autenticar a clientes y empleados con expresiones extremadamente cortas en cualquier contexto.

Requisito mínimo para la autenticación de habla neta: 0,5 segundos
Requisito mínimo para la inscripción de habla neta: 5 segundos

Detección de fraude
Lista de seguimiento: Nuance no limita los tamaños de las listas de seguimiento de los defraudadores, sino que ofrece a los clientes individuales un soporte y orientación personalizados en función de sus situaciones únicas. Dicho esto, nuestros clientes de servicios financieros generalmente mantienen de cientos a miles de listas de seguimiento.

Comparación cruzada
Nuance Gatekeeper incluye herramientas de agrupación de audio para detectar defraudadores a través de la comparación cruzada. **El análisis de agrupación** agrupa muestras de audio similares en función de las características biométricas compartidas de los altavoces internos. La agrupación permite a los equipos de fraude identificar a defraudadores previamente desconocidos, por ejemplo, descubriendo dónde una única llamada está tratando de acceder a diferentes cuentas de clientes. Una vez que se identifica a una persona sospechosa, se puede crear una huella de voz a partir de las muestras de audio y luego agregarla a la lista de seguimiento del defraudador. Los equipos de fraude pueden **realizar búsquedas** retrospectivas para detectar dónde aparece ese defraudador en otros registros históricos de llamadas, obteniendo datos valiosos para fundamentar su caso contra el defraudador y obtener un panorama más claro de la exposición total. A través del motor de biometría de voz de última generación, las herramientas de Nuance permiten a los analistas de fraude realizar agrupaciones eficientes a escala.

Describir un flujo de trabajo típico
Cuando una persona llama a un centro de contacto o IVR, el motor de riesgos Gatekeeper determina en tiempo real si la persona que llama es fraudulenta, basándose en una combinación de comparaciones biométricas (autenticación, detección de listas de seguimiento de fraude), otros factores de riesgo y el riesgo asociado a interacciones anteriores en el recorrido. Si Gatekeeper determina que la llamada es de alto riesgo, se activa una alerta de fraude en tiempo real (mientras la llamada está activa), que puede ser visible para el agente del centro de llamadas y el portal web de Gatekeeper, donde los analistas de fraude administran y revisan los casos de fraude. Debido a la capacidad de Gatekeeper para generar alertas de fraude en tiempo real, las alertas de fraude también pueden usarse para activar la lógica empresarial que, por ejemplo, transferirá la llamada en vivo a una cola de especialistas en fraude capacitados para manejar eventos de fraude. Los agentes del centro de llamadas también pueden activar manualmente las alertas en Gatekeeper si tienen motivos para sospechar que la llamada es fraudulenta según sus procesos empresariales. Estas alertas también aparecerán a los analistas de fraude en el Portal web de Gatekeeper.

El portal web de Gatekeeper es la ventana del analista de fraudes a la actividad fraudulenta en IVR, centro de llamadas o canales digitales. El analista de fraudes puede revisar las interacciones de alto riesgo y comenzar a investigarlas individualmente. Un administrador de fraudes puede asignar interacciones individuales a diferentes analistas de fraudes para su revisión. Dentro de cada interacción, un analista de fraudes tiene acceso a todos los detalles de lo que generó la alerta (puntuaciones biométricas, las decisiones del motor de riesgos de Gatekeeper, así como los metadatos que lo acompañan). También pueden escuchar varias grabaciones asociadas con una interacción determinada para ayudar a concluir si se trató de un intento de ataque fraudulento. Los analistas de fraudes también pueden complementar sus investigaciones utilizando Gatekeeper con información y datos procedentes de otros sistemas a su disposición (por ejemplo, sistemas internos de gestión de cuentas).

Capacidades de detección de ataques de presentación

Nuance Gatekeeper frustra los ataques de presentación mediante el uso de dos tipos de detección de reproducción basada en IA para probar si una muestra de audio representa voz en vivo o una grabación que se hace pasar por un altavoz autorizado. La **detección de reproducción de canal** detecta la presencia de artefactos de señal introducidos por el proceso de grabación y reproducción, y aísla los ataques de reproducción basados en una tasa de falsa alarma definida por el usuario. La **detección de la reproducción de la huella** determina si dos búferes de audio corresponden a la misma expresión. El sistema compara el audio actual con una "huella" guardada de una contraseña de autenticación recopilada previamente. Si las dos huellas coinciden demasiado, la actual se marca como una grabación.

Capacidades de detección de voz sintética

Nuance utiliza la IA para protegerse contra el habla sintética mediante la detección de signos reveladores de grabaciones de voz y artefactos creados durante la transformación de voz, texto adaptable a voz y síntesis de texto a voz de alta calidad.

Enfoque de ajuste, calibración y optimización de implementaciones de usuarios finales

La tecnología de biometría de voz Gatekeeper se utiliza como parte de la toma de decisiones del motor de riesgos. Los modelos incorporados para la biometría de voz pueden proporcionar un rendimiento de alta precisión para la mayoría de los centros de contacto estándar, IVR y aplicaciones digitales. Gatekeeper también cuenta con capacidades para permitir mejoras en línea del rendimiento automáticamente o con una intervención mínima. Por ejemplo, el sistema mejora el rendimiento de la biometría de voz a través de la adaptación de la huella de voz (los perfiles se actualizan automáticamente a medida que se dispone de más datos). Los usuarios del sistema también pueden ajustar los parámetros de Gatekeeper para refinar el rendimiento de acuerdo con los objetivos empresariales. Esto se realiza con la información proporcionada por el portal de informes de Gatekeeper. Los modelos Gatekeeper, ya sea para biometría de voz o el motor de riesgos, se pueden actualizar aún más utilizando datos del entorno de un cliente específico. Esto permite seguir mejorando el rendimiento a medida que el sistema aprende más a fondo las características específicas del entorno (por ejemplo, telefonía, tecnologías de plataforma, población de autores de llamadas). El ajuste se puede realizar sin problemas en segundo plano sin interrumpir un sistema activo.

Interfaz de usuario del agente

Se proporciona una consola de agente lista para usar con Gatekeeper. Esta puede utilizarse de forma independiente o integrada en cualquier escritorio de agente actual como un widget web. Alternativamente, se proporciona una API de REST de agente para permitir que un cliente desarrolle su propio escritorio de agente.

Informes de gestión e interfaz de usuario

Gatekeeper se realiza a través de una interfaz de usuario web. Si una organización utiliza el inicio de sesión único de Active Directory, se puede configurar para acceder a la interfaz web de Gatekeeper, evitando la necesidad de nombres de usuario y contraseñas adicionales. Esto es cierto tanto para la solución Gatekeeper alojada en Microsoft Azure como para la solución local. La capacidad de validación del identificador de llamadas de Nuance Gatekeeper está diseñada e implementada para permitir la extensibilidad mediante la cual ingerimos todos los factores proporcionados por nuestros socios, incluidos los basados en dispositivos y números, junto con los factores que generamos, para proporcionar una evaluación holística del riesgo de una llamada o interacción determinada. Nuance se asocia con Neustar y Smartnumbers, sirviendo a los mercados de América del Norte y Europa.

Detección de anomalías de llamadas

La combinación de capacidades de validación de llamadas, impresión de dispositivos y biometría conversacional trabajan juntas para reconocer el comportamiento anómalo desde el punto de origen (dispositivo) a través de la red de operadores y la integración posterior a la respuesta, ya sea con una persona en vivo o con un actor simulado, como un bot o un discurso sintetizado.

Capacidades de detección

La validación de la red proporciona resultados previos a la llamada, lo que garantiza que las llamadas se realicen desde dispositivos que poseen la ANI especificada, y cuando no, evalúa la probabilidad de suplantación. Estos factores se combinan con todos los demás indicadores disponibles para el motor de riesgos de Gatekeeper al realizar una evaluación de autenticación.

Biometría de comportamiento

(Asociarse con BehavioSec)

Enfoque de toma de decisiones

Subyacente a la plataforma Gatekeeper hay un motor de riesgo de IA que utiliza redes neuronales profundas de última generación para sintetizar la salida de datos de factores biométricos y no biométricos, además de otros datos disponibles, como el historial de autenticación e interacción. El motor de riesgos luego devuelve una decisión (auténtica, fraude) y una puntuación de riesgo general para una sesión o interacción determinada y en todas las instancias de la interacción. Los clientes pueden recuperar los resultados de cada función individual o el resultado agregado mediante programación durante una sesión.

Integración

La plataforma Gatekeeper está diseñada para soportar la integración flexible con los sistemas de los clientes en función de su entorno único y los requisitos de la empresa. Gatekeeper admite la integración con todas las principales plataformas de centros de contacto, incluidos los centros de contacto como servicio (CCaaS) y los sistemas de telefonía locales tradicionales. Gatekeeper también proporciona API para sus funciones principales, así como un SDK para aplicaciones móviles.

Métodos de autenticación y detección de fraude

Todos los métodos de autenticación y detección de fraude que se enumeran aquí se ofrecen como capacidades listas para usar de la plataforma Gatekeeper. Las evaluaciones holísticas de riesgos, los métodos basados en la biometría de voz y en la biometría conversacional y el programa de intercambio de datos de fraude son capacidades internas desarrolladas por Nuance, mientras que la biometría de comportamiento y la autenticación de red se ofrecen a través de asociaciones de OEM con terceros proveedores de tecnología BehavioSec y Neustar, respectivamente.

- **Evaluaciones holísticas de riesgos** a través del motor de riesgos de Gatekeeper basado en redes neuronales profundas que sintetizan factores biométricos y no biométricos, además del historial de interacciones y los datos relevantes de terceros disponibles para autenticar a las personas legítimas y detectar a los defraudadores, independientemente de la identidad o el dispositivo con que se oculten.
- **La biometría** de voz verifica a las personas legítimas e identifica a los defraudadores en tiempo real y después de la interacción en función de su firma de voz única. La autenticación de voz en tiempo real compara la voz de una persona en el centro de contacto, IVR o canal digital con las bibliotecas de clientes conocidos y voces fraudulentas. La comparación de la lista de seguimiento de voz posterior a la interacción compara las grabaciones históricas de llamadas y los intentos de autenticación digital con una lista de seguimiento de defraudadores. Las capacidades de minería de datos, agrupación y búsqueda inversa permiten a los analistas de fraude identificar a defraudadores previamente desconocidos y luego descubrir dónde aparecen en los datos históricos.
- **La biometría de comportamiento** autentica a los usuarios legítimos e identifica actividades fraudulentas en canales digitales respondiendo tres preguntas para cada sesión: ¿Es un ser humano? ¿Es un ser humano bueno? ¿Es el ser humano correcto? El sistema supervisa continuamente el comportamiento del usuario y las señales del dispositivo para verificar a los usuarios conocidos o de confianza, al tiempo que identifica comportamientos sospechosos, anomalías y cambios de sesión para detectar bots, troyanos de acceso remoto, fraude de nuevas cuentas y otras formas de fraude en los canales digitales.
- **La biometría conversacional** verifica a los usuarios y previene el fraude en los canales de mensajería y voz al detectar señales sospechosas en texto escrito o transcrito en tiempo real y a través del análisis posterior a la interacción. De esta manera, es la única modalidad biométrica que puede autenticar pasivamente a los usuarios tanto en contextos digitales como de voz. La biometría conversacional previene formas de fraude difíciles de detectar, como la ingeniería social de asistentes en vivo o agentes de centros de contacto y mulas de fraude contratadas para leer scripts.
- **La autenticación** de red inspecciona las llamadas desde dentro de la red y compara los identificadores de llamadas con una lista de seguimiento de ANI comprometidas conocidas para autenticar llamadas de confianza y detectar suplantación de ANI, llamadas virtualizadas y otras amenazas incluso antes de que lleguen al centro de contacto o IVR.
- **Un programa de intercambio de datos de fraude** comisariado por el Equipo Nuance Fraud Nexus permite a los equipos antifraude detectar a los defraudadores la primera vez que atacan a la organización utilizando huellas de voz y metadatos de defraudadores compartidos por sus compañeros de todo el mundo.

Interacción del usuario final

- Modelo de entrega: El modelo directo es primario por valor de ventas
- Socios: Neustar (validación de llamadas/redes, América del Norte); BehavioSec (biometría de comportamiento, mundial); Smartnumbers (validación de llamadas/redes, Reino Unido/Irlanda)
  Socios de canal: Nuance se asocia con numerosos socios de canal en todo el mundo, incluidos proveedores de centros de contacto como Genesys, Avaya, Cisco y Five9; Microsoft, nuestro socio estratégico en la nube; SI globales que incluyen Accenture y Deloitte; socios de telecomunicaciones que incluyen AT&T y British Telecom; socios regionales; y otros
- Gatekeeper es una solución nativa de la nube que se puede ejecutar en un entorno de nube alojado como SaaS, en nubes privadas y locales, y en el dispositivo a través de un modelo perimetral. Gatekeeper se puede comprar como una solución de plataforma completa o los clientes pueden conceder licencias a las API del motor de biometría de voz central para mejorar sus propias aplicaciones.
- Precios: Precios por niveles, basados en el volumen, por transacción: esto permite que el precio se adapte a diferentes tamaños y volúmenes de implementaciones
- Nuance tiene aproximadamente 1.600 empleados de I + D y 2.350 patentes emitidas (a partir del 9/2020).

Visión y plan

La visión de Nuance es de un futuro verdaderamente sin contraseñas, donde todas las empresas, grandes y pequeñas, aprovechen la herencia asequible y los sistemas basados en la propiedad, proporcionando una experiencia de usuario agradable y eficiente que autentique rápidamente a los usuarios legítimos al tiempo que proporciona una fuerte protección contra el fraude en todos los canales de interacción.

En los próximos años, el mercado de autenticación inteligente se consolidará en unos cuantos proveedores principales en cada geografía, divididos en un subconjunto más pequeño de proveedores que operan en todas las regiones. Tanto los mercados de gestión de identidades y acceso (CIAM e IAM) orientados al consumidor y a las corporaciones dejarán de lado la identidad centrada en el dispositivo para acoger la biometría de voz y de comportamiento como las modalidades principales que los consumidores traen consigo a través de dispositivos y canales. Los equipos de prevención de fraudes continuarán adoptando un enfoque de "queso suizo", aportando soluciones inteligentes que superponen factores biométricos y no biométricos con IA para la prevención y detección en tiempo real, y la utilización de herramientas de análisis biométrico como un componente clave de sus flujos de trabajo de investigación de fraudes.

Por último, los proveedores de IAuth, prevención de fraudes e IAM que no priorizan la privacidad y la ética de los datos en detrimento de las ganancias perderán cuota de mercado frente a los proveedores que adoptan este nuevo paradigma y se posicionan como administradores responsables de los datos de los consumidores.
En este contexto, Nuance será el primero en resolver el desafío central al que se enfrentan todas las iniciativas de identidad digital en todo el mundo: la portabilidad. Proporcionaremos servicios de autenticación de identidad biométrica y prevención de fraudes a todos los consumidores. Nuestra solución unificada y omnicanal pondrá el poder en las manos de los consumidores para autenticarse de forma segura cuando, donde y como sea que interactúen con las marcas y los servicios gubernamentales en los que confían.

Mientras tanto, capacitaremos a los equipos de fraude con una solución unificada que detenga el fraude a través de los canales mediante la detección de atacantes humanos y no humanos basada en evaluaciones de riesgos inteligentes y contextuales con la biometría como elemento central. También nos convertiremos en una figura central que reunirá a equipos de fraude de todo el mundo para unir fuerzas en la lucha mundial contra el fraude a través de un rico consorcio de intercambio de datos y una serie de eventos y liderazgo intelectual.

Principales diferenciadores:

- Nuance Gatekeeper es la única solución que ofrece autenticación biométrica integrada y prevención de fraudes en todos los canales de voz y digitales, lo que permite a las organizaciones agilizar y proteger todo el recorrido de sus clientes a través de una plataforma unificada.
- Nuance Gatekeeper ofrece el rendimiento de autenticación y prevención de fraudes más rápido y preciso del mundo, capaz de verificar a una persona con tan solo medio segundo de audio; capaz de lograr tasas de éxito de autenticación del 99%; y capaz de detectar el 90% de los fraudes con alta precisión.
- Nuance tiene un historial comprobado de implementaciones exitosas de autenticación y prevención de fraudes en todo el mundo con clientes que informan mejores ROI, mayores ahorros en pérdidas por fraude y mayores tasas de éxito de autenticación que las organizaciones que implementan soluciones de la competencia.

SYMNEX

Acerca de SymNex Consulting

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

Sobre Opus Research

Opus Research es una empresa de asesoramiento basada en la investigación que proporciona conocimientos y análisis críticos de las implementaciones empresariales de software y servicios que respaldan las estrategias de atención al cliente y movilidad de los empleados multimodales. Opus Research llama a este mercado "Comercio Conversacional" con cobertura personalizada y análisis del sector que incluye: Autoservicio y Autoservicio Asistido, Procesamiento de Voz y Llamadas, Servicios Web, Asistencia Virtual Personal, Búsqueda Móvil y Comercio y Biometría de Voz.

Para ventas, por favor escriba a info@opusresearch.net o llame al +1 (415) 904-7666.