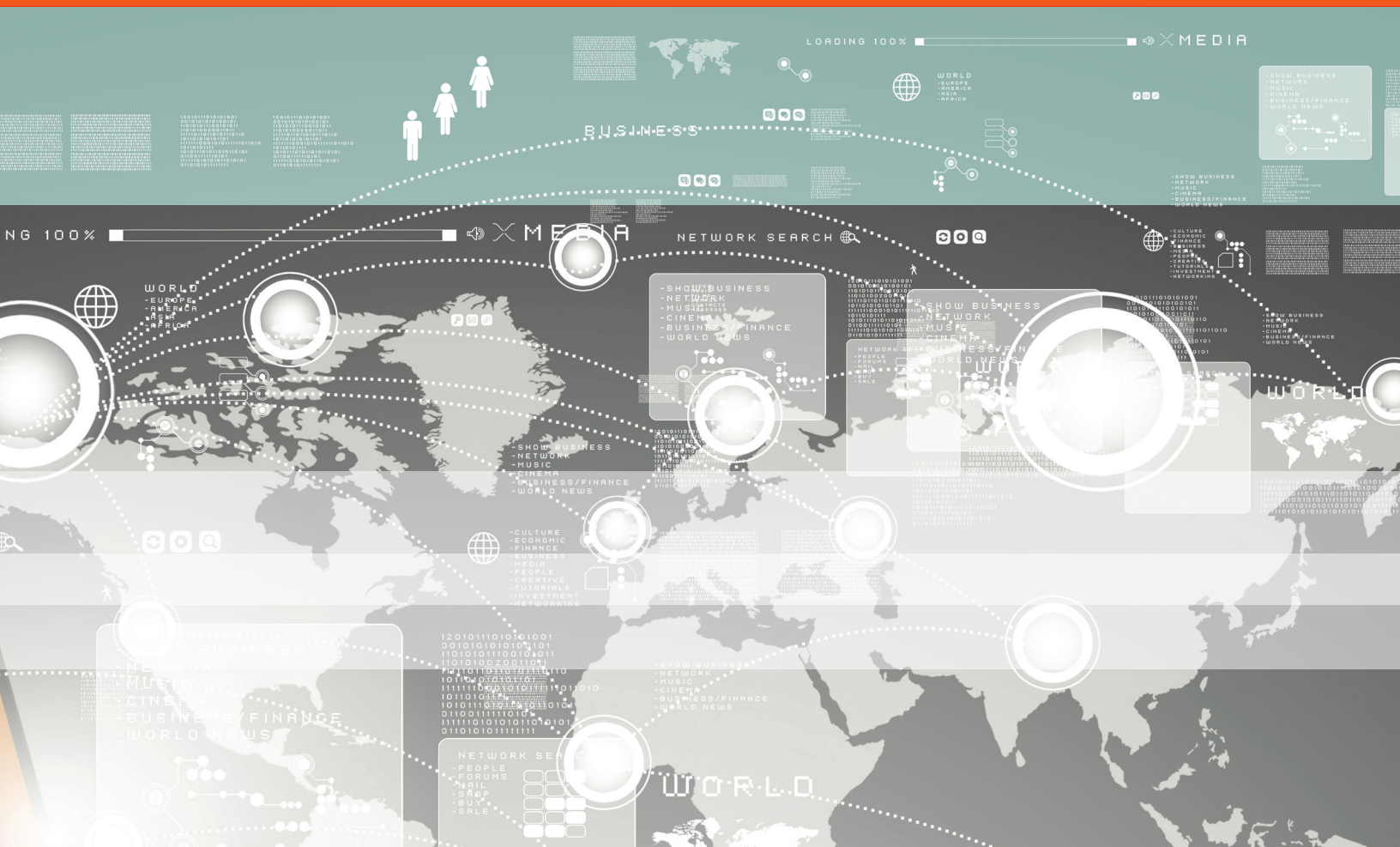
2022 Intelligent Authentication and Fraud Prevention Intelliview

opusresearch



opusresearch | Report »

2022 Intelligent Authentication and Fraud Prevention Intelliview

In this fourth annual Intelliview, Opus Research and SymNex Consulting provide enterprise decision makers with competitive context for evaluating selected solution providers supporting secure customer contact experiences and fraud prevention.

Intelligent Authentication (IAuth) captures a range of products and services that includes biometric factors (voice, facial, fingerprint, behavioral), network intelligence and orchestration used for fraud detection and continuous authentication. This report evaluates 22 solution providers from across the IAuth spectrum who are actively deploying technologies that improve enterprise security, efficiency and customer experience.

January 2022

Matt Smallman, Director, SymNex Consulting
Dan Miller, Founder & Lead Analyst, Opus Research
Derek Top, Research Director, Opus Research

SYMNEX

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

www.opusresearch.net

Table of Contents

Table of Figures

Executive Summary

Requirements for Intelligent Authentication (IAuth) have changed significantly since Opus Research and SymNex Consulting issued our last Intelliview. Billions of people, often in lockdown, routinely use smartphones, tablets or connected computers for banking, e-commerce, telehealth and to avail themselves of government services. Fraudulent imposters have also markedly stepped-up efforts to take advantage of vulnerable authentication strategies.

The 22 solution providers evaluated expand the concept of IAuth beyond voice authentication in Contact Centers or IVRs to support real-time (often passive) use of multiple biometric factors, informed by network intelligence and orchestrated by AI-infused decision engines.

Key highlights include:

- **Solutions Address Authentication and Fraud Prevention:** The same technologies that enable strong authentication can also be deployed for fraud prevention. The transition to modern authentication takes time. Approaches with improved fraud detection can deliver immediate returns and keep fraudsters at bay during transition.
- **Smartphones Play an Expanding Role:** Microphones capture voice, cameras support facial recognition, but that is just the start. Smartphones are highly personal devices that are constant companions for their owners. Possession is a factor in and of itself. The way each smartphone owner inputs information through a screen or places a phone into his or her pocket can help generate confidence scores that individuals are who they claim to be.
- **Voice Biometrics Are Foundational:** The IAuth Intelliview started with providers of solutions that used voice biometrics for caller authentication. Last year's report included companies that added behavioral biometrics and assigned importance to resources that orchestrate the mix of factors to be employed based on the risk associated with an individual and his or her actions.
- **Emergence of Network Authentication and Fraud Detection:** Signaling and other network intelligence data is enabling possession-based authentication and anomaly detection to identify potentially fraudulent calls. Fraud detection and call diversion can take place before a live agent is engaged putting network intelligence to work to establish secure, trusted communication links between businesses and customers.
- **Consumer ID and Access Management (CIAM) Falls Short:** Old-guard "IAM" providers address some of the challenges of digital and mobile security and user authentication, such as registration/enrollment and single-sign on, but they only begin to address core user experience issues that are vitally important for supporting friction free, continuous authentication and fraud prevention.
- **Expect More Vertical and Smaller-Scale Use Cases:** IAuth's core technologies have proven accuracy, effectiveness and ROI at scale in sensitive verticals like banking, insurance, healthcare and government. Solutions now address both security and personalization for retailers, restaurant chains, pharmacies and other verticals with lower volume, lower value transactions.

Modern Solutions for Authentication and Fraud Prevention

IAuth's time has come. Enterprises of all sizes, across a number of vertical industries have found that their traditional methods for customer authentication (primarily PINs, passwords and knowledge-based questions) fall short in terms of security. What's more, customers find them inconvenient, time-consuming and cumbersome. The solution providers evaluated in this Intelliview bring modern technologies and approaches to identify imposters and thwart fraud attempts.

Their services start with biometric engines that can match a person's voice or facial characteristics with stored templates (voiceprints or faceprints) to gauge how confident a company can be that individuals are who they claim to be. That's proven to be a good start, but today's solutions add a wider variety of biometric factors, including behavior, like how they input information on a keyboard.

All can be augmented by "Network Intelligence" and "Device Intelligence." The former describes insights that can be gleaned by evaluating the signals that telephone carriers provide as they complete calls between companies and their customers to assure the number presented is the originator and therefore assure possession in the face of SIM-swap and "spoofing." The latter focuses on device-based techniques, which can create an even more secure key for the enterprise, assuring not just that the user is in possession of that device, but they really are its owner.

Appealing to a Broader Spectrum of Businesses

Large banks, brokerage houses, insurance carriers, wireless and internet service providers and retailers were the early adopters of voice biometrics-based authentication, the precursor to IAuth.

By Opus Research's estimates the firms under evaluation in this document are securing close to 20 billion interactions a year with voice biometrics. In addition, providers of behavioral biometric solutions have installed software on a collective 100+ million devices and, in the aggregate, perform something on the order of another 30+ billion authentication transactions.

The giants of cloud-based contact centers, including Amazon Connect and Google Contact Center AI are accelerating awareness and adoption of IAuth by weaving it into their service offerings.

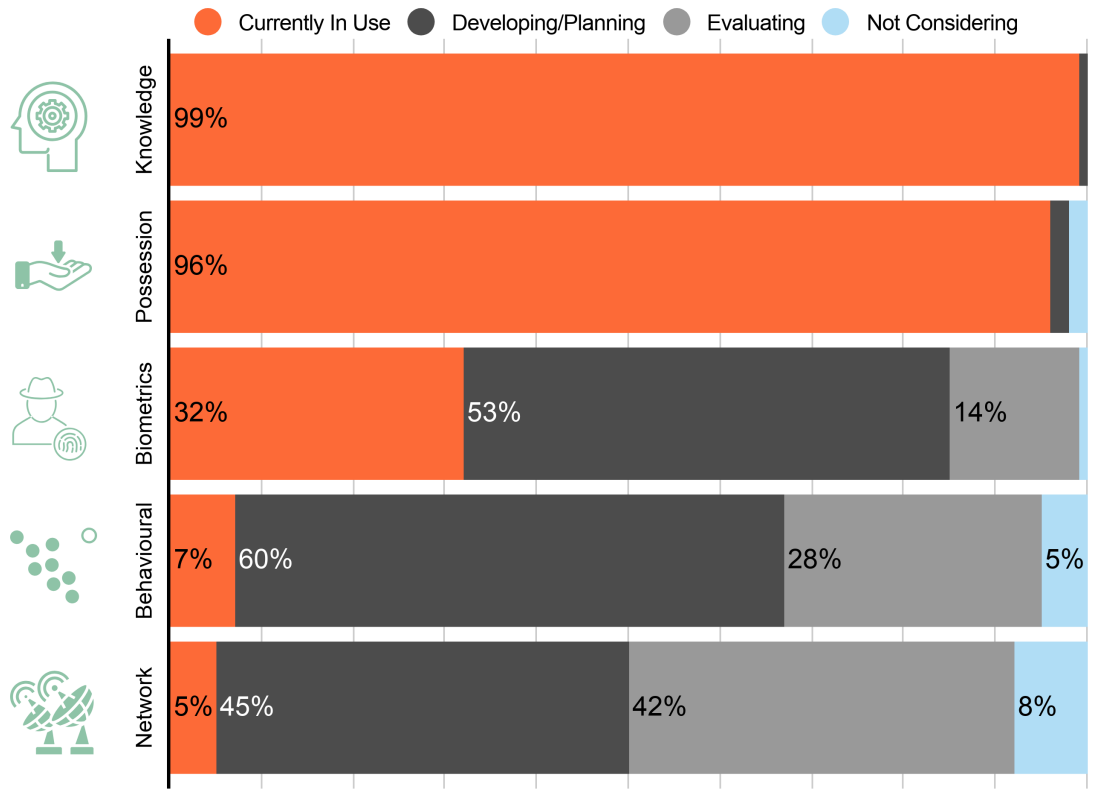
Field Results Show Growing Interest in New Authentication Methods

To better understand the "State of Intelligent Authentication," Opus Research recently surveyed 250 executive decision makers from multiple industries in the U.S., Canada, U.K. and Western Europe about business technologies for security, authentication, and fraud prevention.

When asked about which authentication and fraud detection methods organizations were using we see a wide range of options and multiple factors in use. Survey respondents already mix-and-match a set of authentication and fraud prevention methods solutions.

PINs/Passwords are still the most common, but respondents also incorporate other factors including ANI-matching, out-of-band delivery of one-time-passwords, and knowledge-based authentication via security questions. A growing number are adopting voice and behavioral biometrics, as well as strong interest in developing and evaluating network authentication solutions.

Figure 1: Technology Methods for Authentication and Fraud Detection

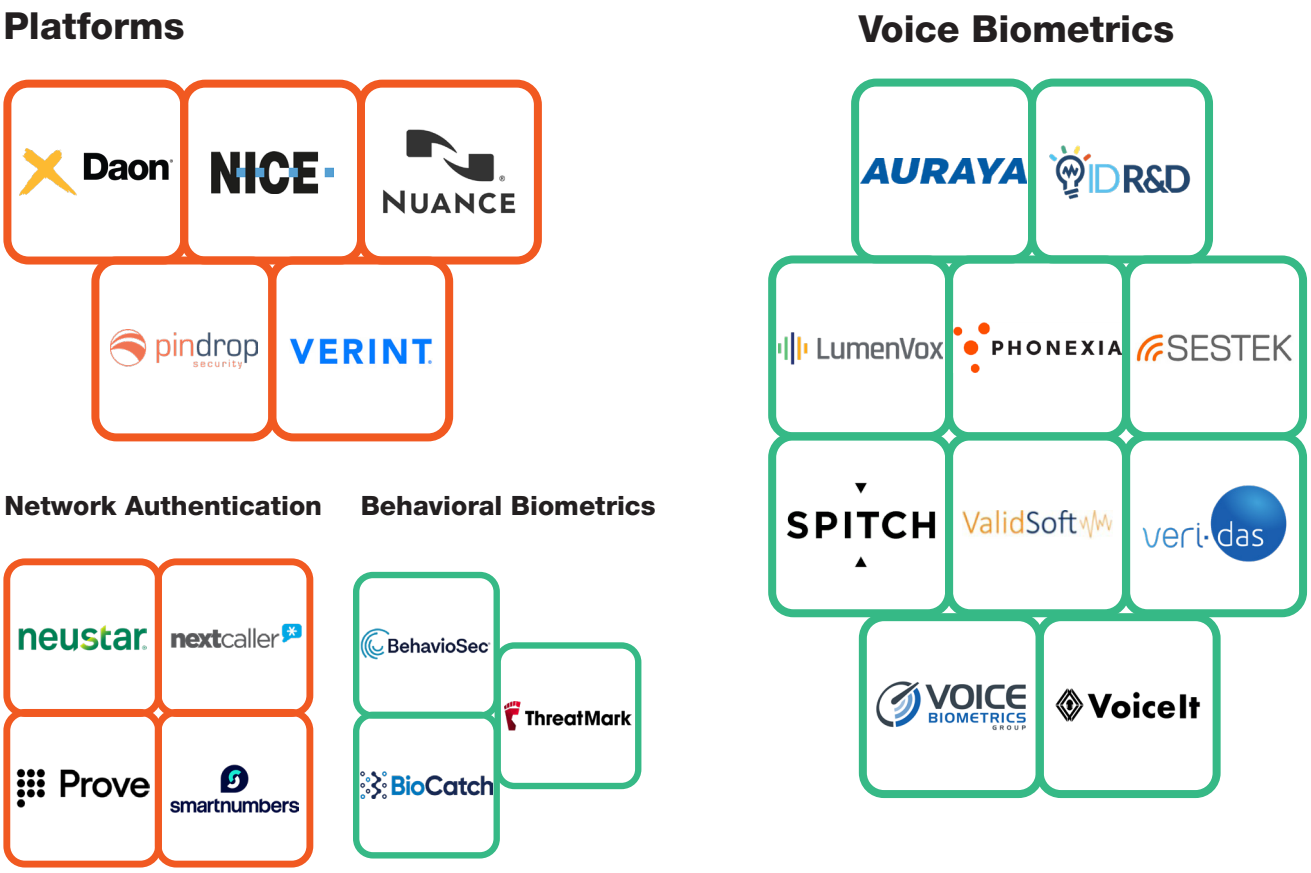


Firms Included in the Intelliview

The firms included in this report do not always compete head-to-head in the marketplace, but each is worthy of consideration as companies seek solution providers that support their strategies for continuous, friction-free authentication or fraud prevention.

This document (Appendix A) provides brief profiles of each company's IAuth offerings and also positions them on an "IAuth Landscape" based on the strength of their product offerings and market positions.

Figure 2: Solution Providers Under Evaluation



Innovation in Voice Biometrics

Short Utterance Text Independent Authentication

Many providers previously competed on accuracy, but we increasingly see that provider performance differences are immaterial to end-user business outcomes. Providers now are focusing their efforts on text independence short utterance authentication performance.

Driven by the demand to use this technology in Natural Language Understanding IVRs without unnatural and hard to enroll passphrases where individual customer utterances are typically less than two seconds. Today, most of these solutions still require far longer enrollment phrases, typically acquired during agent conversations.

Still, some providers are pursuing shorter enrollment audio lengths as well to reduce the agent overhead. Of course, with all things voice biometrics, the trade-off between length and performance may not be quite where every end-user wants it to be, but we expect to see this being an increasing area of focus in the next year.

"VOICE BIOMETRICS HAS ALREADY PREVENTED MORE THAN 1000 ACCOUNT TAKEOVERS AND IS SAVING US MORE THAN 40 SECONDS PER CALL ON AVERAGE."

—Director of Fraud Prevention, Multinational Banking Corporation

---

Cloud Contact Center

The pandemic driven requirement to enable home working has accelerated the transition to cloud contact centers for many enterprises. Whilst the priority has been getting those services up and running with minimal disruption, we see an increasing number of enterprises starting to take advantage of the increased flexibility of these solutions.

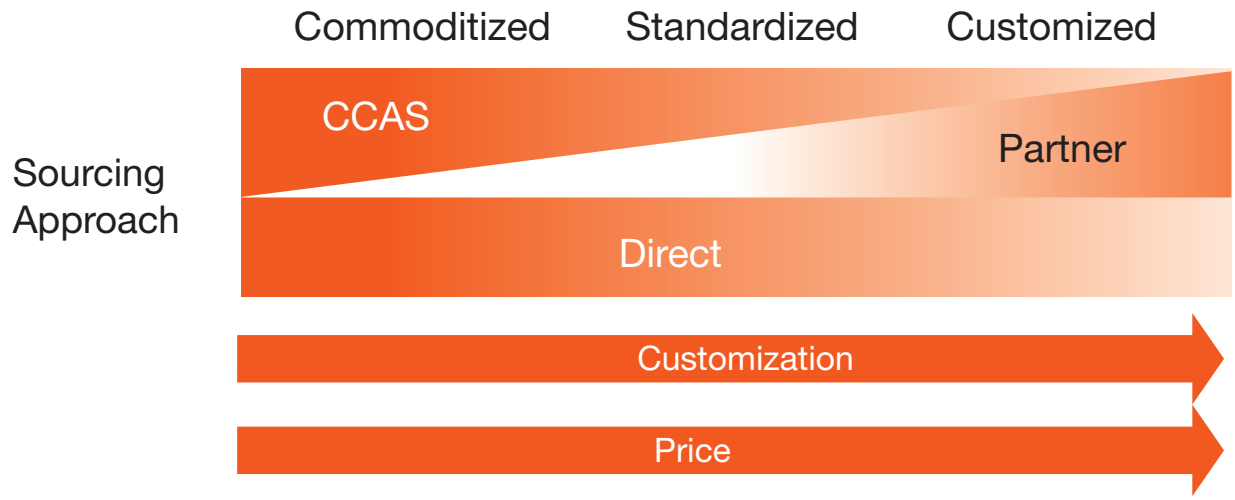
Many organizations that lifted and dropped their existing knowledge-based authentication processes onto these platforms are now beginning to look at more modern security approaches such as voice biometrics. These are now significantly more accessible as a result of the standardized integrations on these platforms and increasing availability of cloud-based voice biometrics services.

Market Stratification

We see an emerging stratification of the voice biometrics market, particularly as it relates to contact centers. At the highly customized end of the market are the major platform providers Nuance and Pindrop, focusing on Authentication and Fraud Prevention. These solutions are highly customizable, backed up by extensive professional services teams and can be made to work with any underlying telephony platform.

Closely related to these are the integrated solutions from Verint and NICE. Where customers already use part of their respective suites, the significantly reduced implementation overheads make them a logical first consideration. While not yet as widely fielded, these solutions are similarly customizable but have the significant advantage of lower implementation cost and complexity (after initial implementation of the suite). We expect to see substantial growth from these players as their extensive installed base realizes the opportunity of improved authentication and fraud prevention.

Figure 3 - Voice Biometrics Market Stratification



At the commodity end of the market, Amazon and Google have defined a very low price point at 1-2c per authentication, but with minimal opportunities for customization, as yet unknown performance and availability restricted to their own or partners platforms. It remains to be seen which, verticals and use cases, these solutions will be good enough for, but we expect the availability of these services to pique enterprise interest even if they subsequently choose alternatives for implementation. Whilst Amazon and Google may have built their own technologies, most cloud contact center providers do not have that luxury. Still, to remain competitive, they are increasingly white labelling or offering tight integration with other specialist providers in this Intelliview.

In between these two poles, we see the majority of voice biometrics providers with more standardized offerings. Without enormous professional services teams, they are generally focused on integrating with a handful of telephony platforms (such as Auraya's EVA solution for Amazon Connect, ValidSoft's partnership with Five9, Talkdesk (white labeled) and Vonage, and VBG's with Aspect) which reduces implementation complexity and allows them to focus on the core of the solution.

We expect this market section to see the most activity in the next few years as voice biometrics becomes desirable and accessible to a far wider range of organizations. Vendors targeting this section need to focus on the volume of deployments, not their individual scale and ensure that their customers achieve the business and technical outcomes they are seeking. It's telling to note that both Nuance and Pindrop are enhancing or supplementing their solutions to cater to this market.

Access and Availability – "Click to start"

The underlying machine learning and signal processing of voice biometrics might require PhDs and years of experience to understand, but the core integration and implementation mechanisms are relatively simple. Most developers can understand the basic concepts in less than an hour. It's promising; that some providers are making their solutions easier to get started with. We expect this to reduce the uncertainty and perception of complexity around these solutions that have inevitably held many organizations back from progressing.

Amazon makes their VoiceID service for Amazon Connect available to anyone with a credit card to try, and it's becoming increasingly easy for developer-focused organizations to get started with voice biometrics. Auraya's EVA solution, also for Amazon Connect, is available from the AWS marketplace with CloudFormation templates that stand up all of the required infrastructure for a production implementation alongside a clear and transparent pricing. VoiceIT's co-pilot program provides rapid access to a Sandbox environment alongside their extensive example code on GitHub and easily accessible API references. VBG's similarly developer-focused offering offers 60–90-day free trials and pay as you go options right from their website. Phonexia provides developers with a sandbox, and Veridas publishes all of their APIs on their website. Nuance can also provide their cloud Gatekeeper platform on request and ValidSoft's cloud-based sandboxes are available on demand either direct or pre-integrated with their partners.

Integrating Analytics and Intelligence into Platforms

Our platform respondents solutions have matured over the last year becoming increasingly comprehensive, integrated and easy to implement.

Speech Analytics

Speech analytics is now almost universal as an optional component of these platforms with varying degrees of integration. This technology can be used to identify callers using word patterns indicative of fraudster scripts, attempting to socially engineer agents or agents acting out of compliance. With dedicated speech analytics products in their portfolio, NICE and Verint's implementations are probably the most versatile. Still, Nuance's security-focused Conversation Print is arguably the most tightly integrated with fraud detection, seeing significant success with challenging issues such as refund abuse. We expect to see this as an increasingly important part of holistic IAuth solutions in the future.

AI-Infused Analytics for Fraud Detection

As the range of data points available to platforms increases, the permutations and combinations of outcomes from different methods is increasingly hard to plan for. Pindrop has always produced a single risk-based score from their numerous fraud detection methods. Now, Nuance's is using AI in their Risk Engine to optimize business outcomes based on all available authentication and fraud detection methods. We're still not sure whether all end users will be comfortable with this level of abstraction. Still, for the majority, this trend dramatically simplifies the planning and implementation of these technologies.

Trusted Agent

Covid accelerated many transformations, including remote, distributed and work from home operations. This has also increased potential risks associated with the remote contact center agent. Several providers including ValidSoft, Nuance, Verint and VBG recognized this need and were quick to bring bespoke solutions to market that continuously authenticate remote agents to prevent handover to unauthorized proxies acting on behalf of the genuine agent. As regulators catch up with these changes in working practices we expect demand for these solutions to increase significantly.

Network Intelligence

All platform respondents increased the importance of Network Intelligence solutions this year, recognizing that not all callers are likely to be in the scope of technologies such as voice biometrics. Pindrop's acquisition of Next Caller on top of their existing capabilities was perhaps the boldest move, but Nuance's partnership approach also gained traction, and Verint is bringing the capability into its Adaptive Fraud solution. We see significant value in these types of solutions not just as part of a platform but as solutions in their own right (see below) for lower risk verticals and use cases. As a result we expect to see the use of this data quickly become table stakes for a platform solution whether through partnerships or in-house solutions.

"ONCE ANI SPOOF DETECTION WAS IMPLEMENTED, FRAUD ACTIVITY DROPPED SIGNIFICANTLY AND HAS BEEN STABLE FOR 4+ YEARS"

—Product Manager, Global Financial Holding Company

Integration

As a CCaaS provider in its own right, we were happy to see NICE finally bring its Real-Time Authentication solution to CXone, providing the most comprehensive own brand solution of any CCaaS provider. At the same time, Nuance and Pindrop increased the depth and sophistication of their integrations with other cloud platforms such as Amazon Connect and Five9. They also improved the ease of integration with more traditional on-premises platforms. It's increasingly easy to get started with these platforms, every respondent now has some form of SaaS offering to evaluate their effectiveness with real-world data without months (and sometimes years) of expensive implementation effort. Many of our respondents' traditional customers are evaluating or moving to CCaaS solutions requiring providers to develop new and enhance existing integrations. We expect increased availability and lower cost of ownership to make these solutions relevant to a broader market than today.

Introducing Two New IAuth Categories

The IAuth market continues to evolve, and we're excited to include two new categories alongside voice biometrics technology and platforms this year:

Network Authentication and Fraud Detection

Network Authentication and Fraud Detection uses signaling and other Network Intelligence data to increase confidence that the presented number is the one it claims to be. They enable possession-based authentication and anomaly detection to identify potentially fraudulent calls. Smartnumbers, Neustar, Prove, and Next Caller protect more than 5 billion customer interactions, and similar technology is also leveraged by platform solutions from Nuance, Pindrop and Verint. These solutions provide an easy first step for many organizations towards IAuth without the more complex integrations and enrolment requirements of voice biometrics.

Network Authentication solutions increase the confidence that the ANI associated with a call has not been spoofed or recently switched to a new device so that, subject to matches in enterprises records, the presented number be used to authenticate callers for lower-risk transactions. For those calls that don't match or have some anomalies, these solutions use their understanding of typical and known fraudulent routing patterns to assess the risk that the call is fraudulent and treat accordingly. Next Caller, for example, has so far mapped more than 3 million unique routes. Key features we evaluated at included:

- **Spoofing Detection** - The ability to detect whether the presented ANI or CLI is genuine or has been spoofed.
- **Call Routing Risk Assessment** - The ability to identify network routes that are more likely to be associated with fraudulent activity.
- **Watchlist and Velocity Detection** - The ability to detect known fraudulent originating devices and suspiciously high frequency calls from other devices.
- **Device Change/SIM Swap Detection** - The ability to detect if a presented number's originating device has recently changed or been ported to another device or network.
- **Case Management** - Tools to allow fraud analysts to investigate suspicious calls, including providing feedback to improve future solution performance
- **Integration** - Some solutions are deeply integrated with certain carriers or come from providers with privileged network access, which, whilst providing significant benefits, may constrain their application in other contexts.

"THE PROJECT GOAL WAS STRAIGHT FORWARD, REDUCE CUSTOMER FRICTION WHILE MAINTAINING THE INTEGRITY OF OUR FRAUD PREVENTION … THE RESULTS (OF BEHAVIORAL ANALYTICS) EXCEEDED EXPECTATIONS AND PERFORMANCE CONTINUES TO REMAIN STABLE."

—Director of Lending, U.S. Regional Lending Services Firm

Behavioral Biometrics

Behavioral biometric providers support techniques for companies to detect imposters or authenticate genuine customers based on the unique way individuals interact with their devices, including how they hold their smartphone or whether they use two thumbs or their index finger to type. As a growing amount of human commerce is carried out online or over mobile devices, and "zero knowledge", anonymity and pseudonymity are taking hold, behavior-based analysis assigns risk scores to individuals or devices based strictly on their actions, in comparison to known behaviors, or those of known imposters.

Three firms - BehavioSec, BioCatch and ThreatMark - responded to our requests for information. Each distinguishes itself by taking a unique approach to detecting anomalous traits that indicate heightened risk that an individual is behaving like an imposter, rather than an authentic customer or prospect. We foresee their technologies taking on heightened importance as the use of IAuth expands to companies who want to detect potential fraud that's initiated by individuals who contact a company infrequently or for the first time.

Intelliview Maps

To assist decision makers in evaluating competing solutions providers, Opus Research represents their positioning in a series of "Intelliview Maps. In reference to Figures 4, 5, 6 and 7 that follow, we have arrayed the solution providers to relative market positioning and success. The size of the ovals on the Intelliview reflect two, all-important factors:

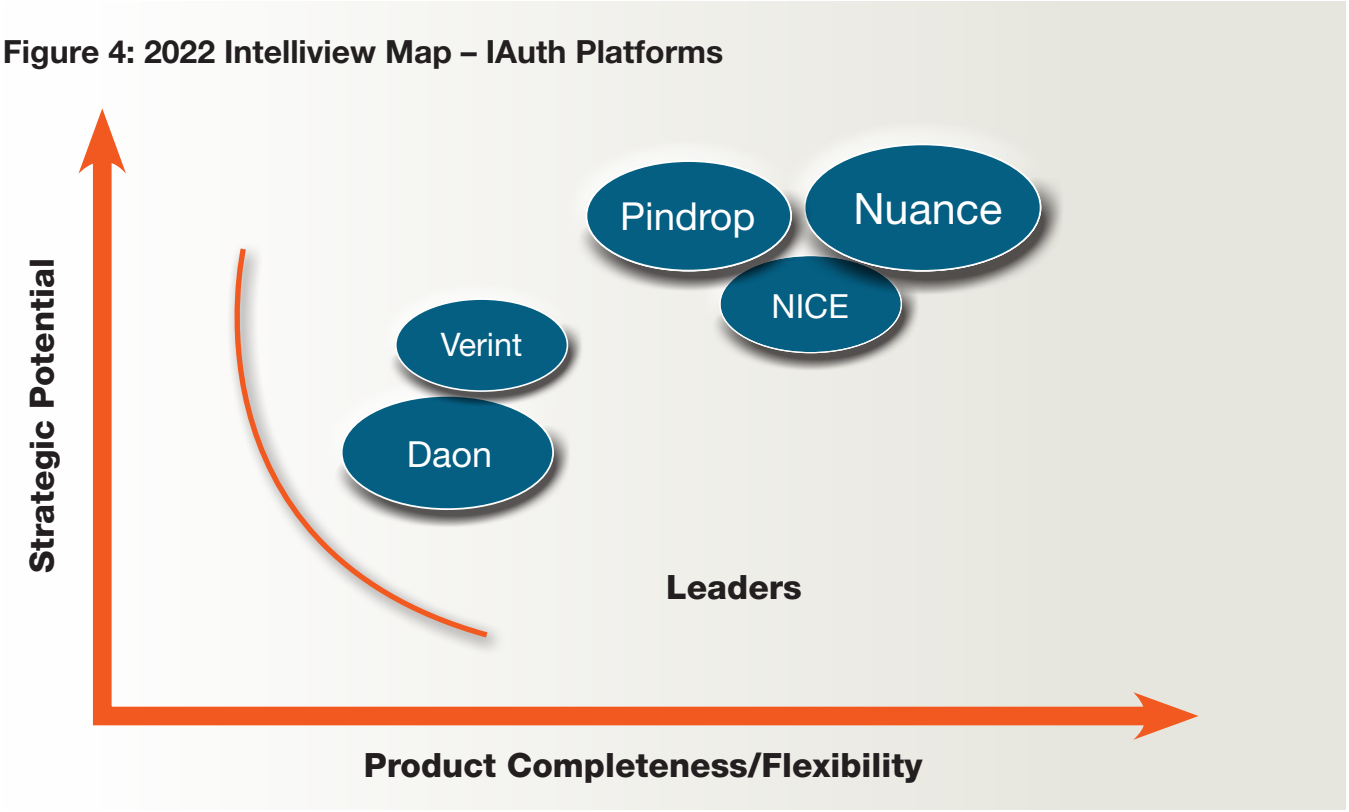
- **Product Completeness/Flexibility** – captures how current product capabilities meet real customer requirements as evidenced by referenced implementations. It includes an assessment of flexibility to adapt to specific needs as demonstrated by reference customers. Platform providers receive the highest assessment when their capabilities are "broad". Their services and features generally cover all columns of the solutions stack: Authentication, Fraud Prevention, Orchestration and Applications. Core Technology providers receive the highest assessments when their capabilities are "deep". This includes external validation of performance, strategies to mitigate common vulnerabilities, availability and quality of API documentation and low effort approaches to tune and calibrate the core technology across a wide variety of both authentication and fraud detection use cases.

- **Strategic Potential** – captures how vision and roadmap appeals to current and evolving technology requirements in contact centers and beyond. It includes an assessment of each company's ecosystem of go-to-market partners and integrators. Platform providers receive the highest assessments when they can demonstrate broad compatibility with a broad range of factors and telephony platforms. Core Technology providers receive the highest assessments when they can demonstrate continued investment in performance improvements and product evolution.

The size of the ovals represents each provider's market impact based on company-provided or publicly available information of customers, interactions secured, and users enrolled. It is modified by an assessment of current financial strength (revenue, profitability, financial backing, longevity and size of customer base).

Platforms

Figure 4: 2022 Intelliview Map – IAuth Platforms



Leaders (in alphabetical order)

Each respondent in this category earns their place in the Leader segment by distinguishing themselves in one or more areas of our analysis. In practice, the right solution for any enterprise is dependent on factors including the value at risk, scale and complexity of the organization and existing technology investments. Still, all of this year's respondents deserve consideration.

Daon

Daon's achieved its leadership role by focusing on its IdentityX solution. It supports a wide range of biometric and alternative authentication mechanisms for digital onboarding and continuous authentication. It allows organizations to mix and match the most appropriate mechanism across contact center, in-person and mobile use cases that span Financial Services, Travel & Hospitality, the Public Sector. Taking an approach that it refers to as "Identity Continuity", Daon supports a vision for applying the appropriate biometric or authentication factor that starts with onboarding and then encompasses authentication on-device or through contact center resources.

NICE

NICE's Real-Time Authentication (RTA) uses their platform's deep integration with the contact center to provide a compelling authentication and fraud prevention solution to their existing customers. By accessing historical recordings, RTA can pre-enroll callers and proactively identify fraudsters from scanning hundreds of thousands of calls to deliver business value on day one of implementation with minimal additional effort. Authentication and fraud

prevention outcomes are displayed using their existing agent desktop and back-office tooling, requiring little extra training or education. NICE's complimentary "Enlightened fraud prevention" solution based on their Nexidia speech analytics can identify anomalous and fraudulent behavior. These capabilities are also available out of the box for customers of NICE's contact center platform CXone.

Nuance

Nuance continues to dominate the market with by far the largest number of implementations and annual authentications. Their cloud-based Gatekeeper solution is winning new large enterprise and mid-market customers and migrations from existing on-premise implementations. The solution itself continues to evolve, with new features being made regularly available. Nuance's Lightning voice biometric engine continues to push the performance envelope delivering high confidence from the short utterances typically found in IVRs (another big part of Nuance's business). They are now focused on being able to enroll users with similarly short utterances reducing agent registration requirements. On the fraud prevention side, Nuance continues to invest in tools to improve the analyst experience and share knowledge and expertise through their Fraud Nexus center of excellence. On the horizon, Nuance's AI Risk Engine aims to simplify the management of thresholds and combinations when multiple authentications and fraud detection factors are in use by focusing on business outcomes.

Pindrop

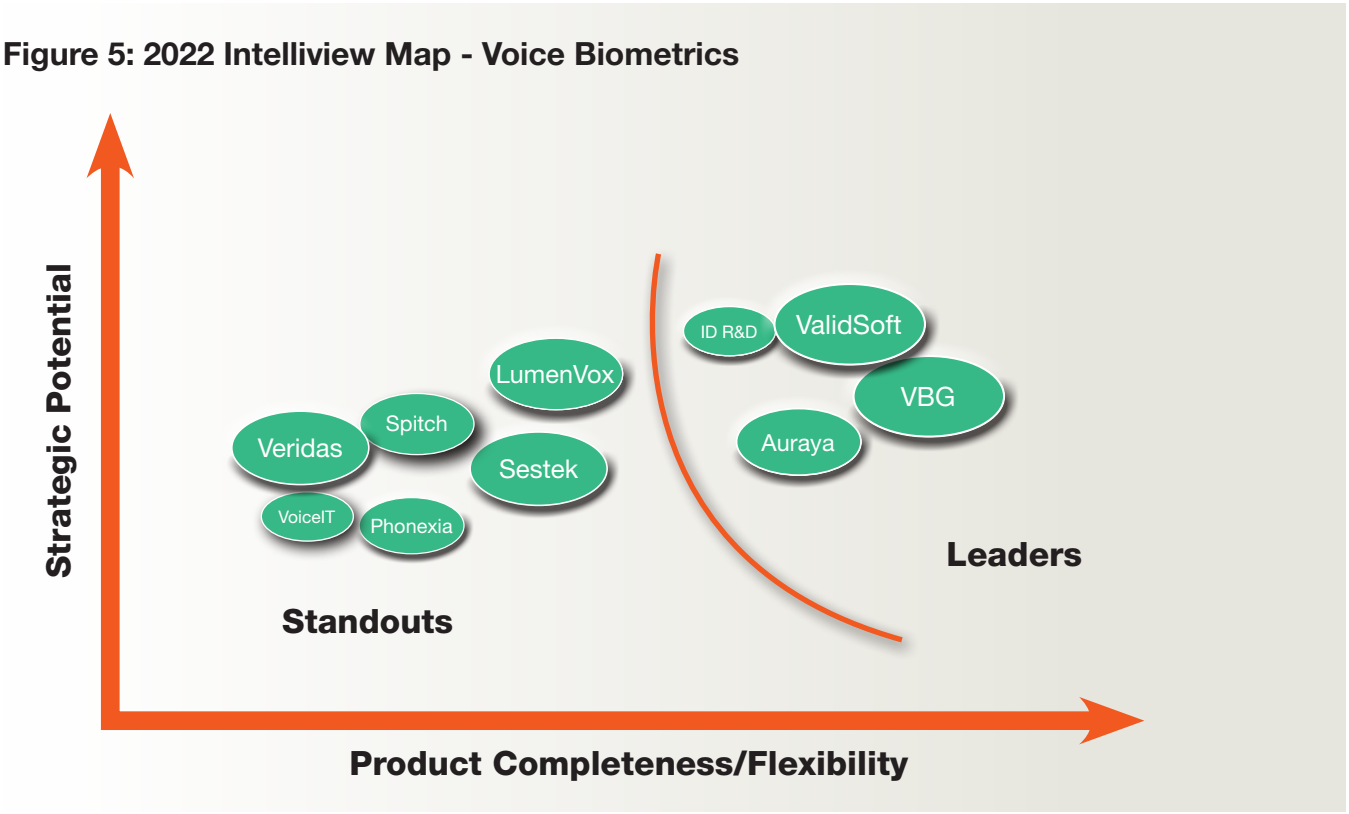
Pindrop's historical focus on fraud prevention continues with best-in-class analyst experience and new tools to predict which accounts are most at risk in advance of any loss. Their phoneprinting technology and consortium data now covers almost 5 billion calls and 2 million fraud events. Their passport voice biometrics-based authentication solution has been updated with version 3 of their Deep Voice algorithm, promising even quicker and more accurate authentication results. The cloud-based solution is now available in Europe for the first time. Pindrop's acquisition of Next Caller (also listed separately under Network Authentication and Fraud Detection) strengthens their existing caller ID validation services and consortium data. It also makes Pindrop solutions relevant for a far wider proportion of the market.

Verint

Verint's extensive portfolio includes two solutions. Adaptive Fraud is a comprehensive solution based on the insight gained from operating one of the largest hosted IVRs in North America and backed up by an experienced team. It includes behavioral analytics and network intelligence capabilities to identify fraudulent calls alongside their Sentry watchlist, which identifies at-risk accounts enabling customers to achieve risk-based self-service and call routing. Identity Authentication and Fraud Detection using voice biometrics is rooted in their call recording technology and tightly integrated with their agent desktop and back-office applications making it very easy to implement and a logical consideration for existing customers. Verint's speech analytics technology can similarly identify suspicious behavior and trigger appropriate after call responses.

Voice Biometrics

Figure 5: 2022 Intelliview Map - Voice Biometrics



Leaders (in alphabetical order)

Our market leaders distinguish themselves through the clear link between their extensive implementation experience, mature solutions and deep focus on voice biometrics or authentication.

Auraya

Auraya's extensive implementation experience with their ArmorVox suite shines through in their EVA solution. EVA wraps essential user interface and business logic around the ArmorVox engine to speed implementation. This solution incorporates authentication and fraud detection in a packaged solution that can be up and running in a few clicks with transparent pricing when implemented in AWS. EVA's ability to efficiently crossmatch millions of calls alongside their per speaker background models are standout features.

IDR&D

IDR&D is principally focused on the application of Face and voice biometrics to mobile device use cases. Their focus on high-performance voice biometrics, particularly in defeating presentation attacks alongside the increasing traction in their target markets, earns them a space in the Leader's category. They should be included in any evaluation of voice biometrics for novel use cases.

ValidSoft

ValidSoft stands out with their emphasis on privacy-by-design and compliance with tough European privacy seal standards. Significant Fortune 50 wins have recently recognized ValidSoft's deep technical expertise. They earn

their space in the Leaders category because of these wins and their demonstrably strong partnerships with Five9, Talkdesk, Vonage and others, driving increased adoption. ValidSoft core technology can be packaged in every conceivable implementation mode, including their own hosted solution and embedded/on-device applications.

Voice Biometrics Group (VBG)

VBG is second only to Nuance in the number of pure voice biometrics deployments. With an exclusive focus on this market, their solution continues to evolve with equal emphasis on core engine performance and user experience/ business outcomes. We were particularly impressed by the administrative user interface that clearly reflects lessons hard-won from implementation experiences. They have a remarkably diverse and increasingly global client base ensuring that most conceivable use cases or requirements can be met with a wide range of implementation models (including hosted cloud) available. One client reported, "Their responsiveness and willing to be flexible with state-of-the-art technologies is unprecedented."

Standouts (in alphabetical order)

There are, of course, far more technology providers that we could show here. Still, each respondent in this category has unique attributes that make them exceptionally well suited for some use cases and markets. Given their trajectory, we expect several to be future leaders hence the "ones to watch" moniker.

LumenVox

LumenVox's pedigree as one of the pre-eminent speech recognition providers provides a strong foundation for their voice biometrics solution. As the result of their merger with VoiceTrust in 2018, their text-dependent and text-independent solution are used by several systems integrators and solutions providers. Their packaged password reset solution solves a surprisingly big problem for large enterprises and continues to prove popular. One partner reported, "There is a mutual respect and support for each other's offering, and we continue to collaborate on new opportunities in our market."

Phonexia

Phonexia's long experience with voice biometrics and speech recognition for public safety use cases provides a solid foundation for their commercial offering. Providing only text-independent solutions, their sandbox can be stood up for testing in a matter of hours. Judging by the number of evaluations underway and the solutions capability, it won't be long before they win significant business in their target markets. Their modern engine is optimized for short utterance authentication, and we are particularly impressed by the results they have obtained given their short time in this market.

Sestek

Sestek is the leading supplier of speech solutions of all types in Turkey and the Middle East. As Turkey has more voiceprints in use per capita than any other country globally, it's not surprising that their solutions are particularly mature and able to win clients against entrenched incumbents suppliers. Their client base includes leading financial services and telecoms operators in their target market. Their solution covers authentication and fraud prevention use cases and can be deployed in mobile applications or contact centers alongside their conversational AI platform.

Spitch

Based in Zurich, Spitch focuses on a range of speech solutions, including virtual assistants and speech analytics, particularly for languages other than English. Their success with voice biometrics in the notoriously challenging Swiss marketplace (where most organizations need to support three different languages and comply with some of the most stringent privacy legislation) with banks and others is a testament to their perseverance and technical capability. Their text-independent solution includes fraud detection but can also be integrated with their speech analytics product to detect new fraudsters through their use of scripted or anomalous language.

Veridas

A new entrant in this year's Intelliview, Veridas focuses entirely on document recognition, voice and facial biometrics for authentication, fraud prevention and identity proofing use cases. Based in Spain, they have significant traction in Spanish speaking markets but are seeing increasing success elsewhere, including a high-profile win at Deutsche Telekom for their voice biometrics solution. Their APIs and performance data are available to anyone on their developer-focused website.

VoiceIT

VoiceIT was the original SaaS provider of voice and face biometrics. Whilst staying true to their developer-focused roots with publicly available APIs and code samples, they are now adding text-independent authentication to their solution. Their "Co-Pilot" onboarding program provides a step-by-step process that ensures developers get the support they need and can quickly navigate the privacy and calibration challenges of the technology.

Cloud Providers

Not shown on an Opus Research Intelliview chart above but included for completeness, the cloud computing giants have also entered the voice biometrics market with disruptive and commoditized solutions.

Amazon

Amazon's VoiceID service entered beta in January 2021 and became generally available in September 2021, adding watchlist based fraud detection to the existing authentication use case. The text-independent solution only works with Amazon Connect. Still, for users of the platform, the integration is impressively easy to implement, and at 2.5c per transaction (enrolment and authentications), the price is very competitive. After a quick onboarding process, VoiceID components can be dropped on existing call flows, and agents can complete all required enrolment and authentication actions using the standard interface. There is, as yet no mechanism to calibrate or evaluate the performance of the underlying biometric model, so its real-world applications may be limited to lower risk use cases.

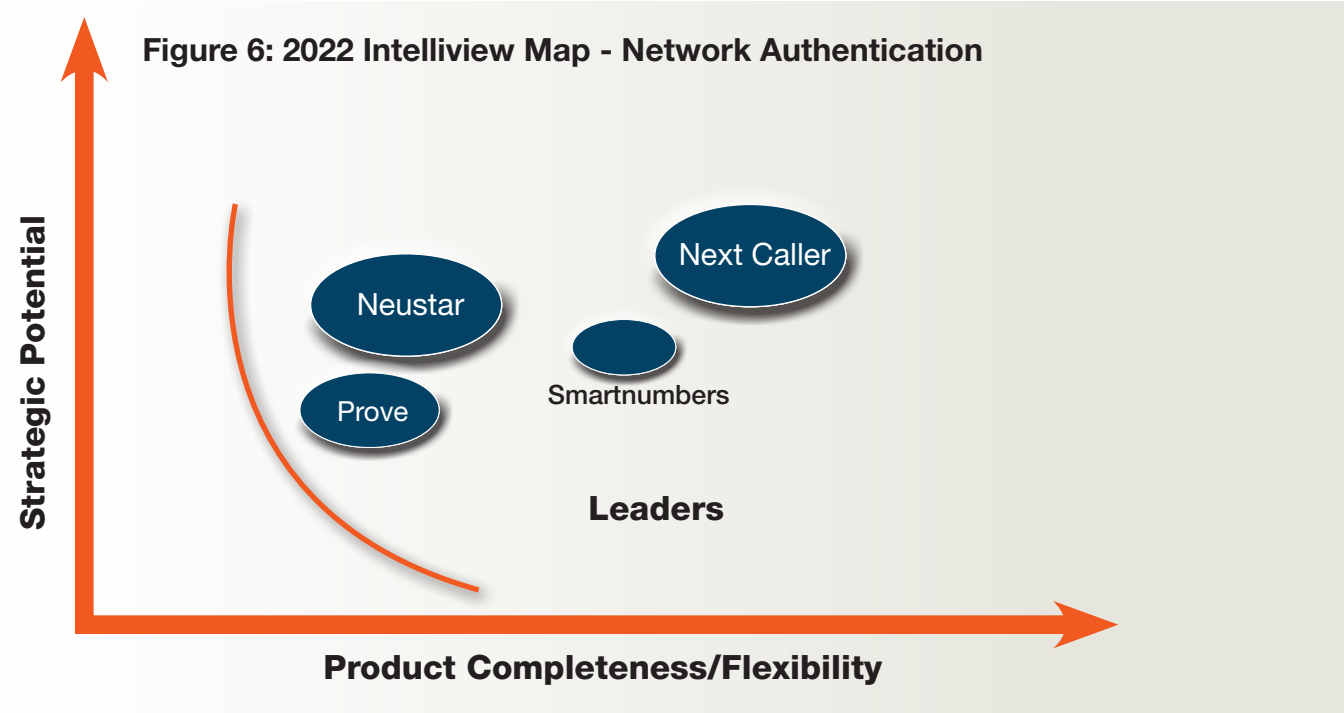
Google

Google announced Speaker ID as part of their Contact Centre Artificial Intelligence (CCAI) proposition in Oct 2021. The solution is only available through partners (including Genesys and Avaya), and there is no publicly available documentation, so it is difficult to draw too many conclusions. What is clear is that the initial implementation is likely to be closer to text prompted than true text-independent and limited to Google's Dialogflow natural language solution. Nonetheless, Google's announcement further validates how essential voice-based authentication is to these type of solutions and undercuts Amazon's at 1c per authentication.

Microsoft

Microsoft's Speaker Recognition service is part of the Azure Cognitive Services. Whilst the API has been available in preview for several years, it recently added text-independent features and was made generally available in November 2021. The bare-bones API is provided with code samples in every conceivable programming languages. It supports both text-independent and dependent use cases for identification (up to 50 candidates so could also be used for limited fraud watchlists) and authentication. At between 0.5c - 0.3c per transaction, depending on volume, it's exceptionally competitively priced. Like all big cloud services, it simply provides a numerical score that is up to end-users to determine whether is sufficient confidence for their use case. Microsoft also insists that enrolled users speak a specific activation phrase at the start of their enrolment. While effectively navigating the privacy challenge, it is likely to be challenging to implement in call center scenarios.

Network Authentication and Fraud Prevention



Leaders (listed alphabetically)

The market for Network Authentication and Fraud Prevention includes many more firms than our respondents. Still, all our respondents earn their spot in our market leaders category by demonstrating market traction, technical capability and strategic promise.

Neustar

Neustar's solutions combine their TRUSTID acquisition in 2019 and their status as the provider of the majority of the US's Caller ID infrastructure. They form part of the business being acquired by TransUnion. Neustar Inbound Authentication includes their patented pre-answer authentication technology allowing high-risk calls to be treated differently before they even connect with the end user's infrastructure. Their privileged carrier status allows them to confirm the claimed device is actually in use. When not a unique device, they use their experience of billions of calls to assess the risk of spoofing. It can be further integrated with their OneID database solution to identify the owner of unknown ANIs, increasing identification and subsequent authentication rates.

Next Caller

Acquired by Pindrop in March 2021, Next Caller complements Pindrop's wider platform and continues to operate as a separate company, so they are included in this category in its own right. Next Caller's VeriCall solution covers billions of calls annually and has catalogued millions of unique carrier paths. VeriCall provides a trust score with reason codes reflecting a wide range of risk factors based on signaling data through a speedy API call allowing end-users to make appropriate routing and treatment decisions depending on the outcome and trusting the Caller ID for authentication when appropriate. One customer we spoke to described their relationship with Next Caller as "very positive" and had seen improvements in authentication rates year on year with no increase in fraud. The solution is available in markets outside the US.

Prove

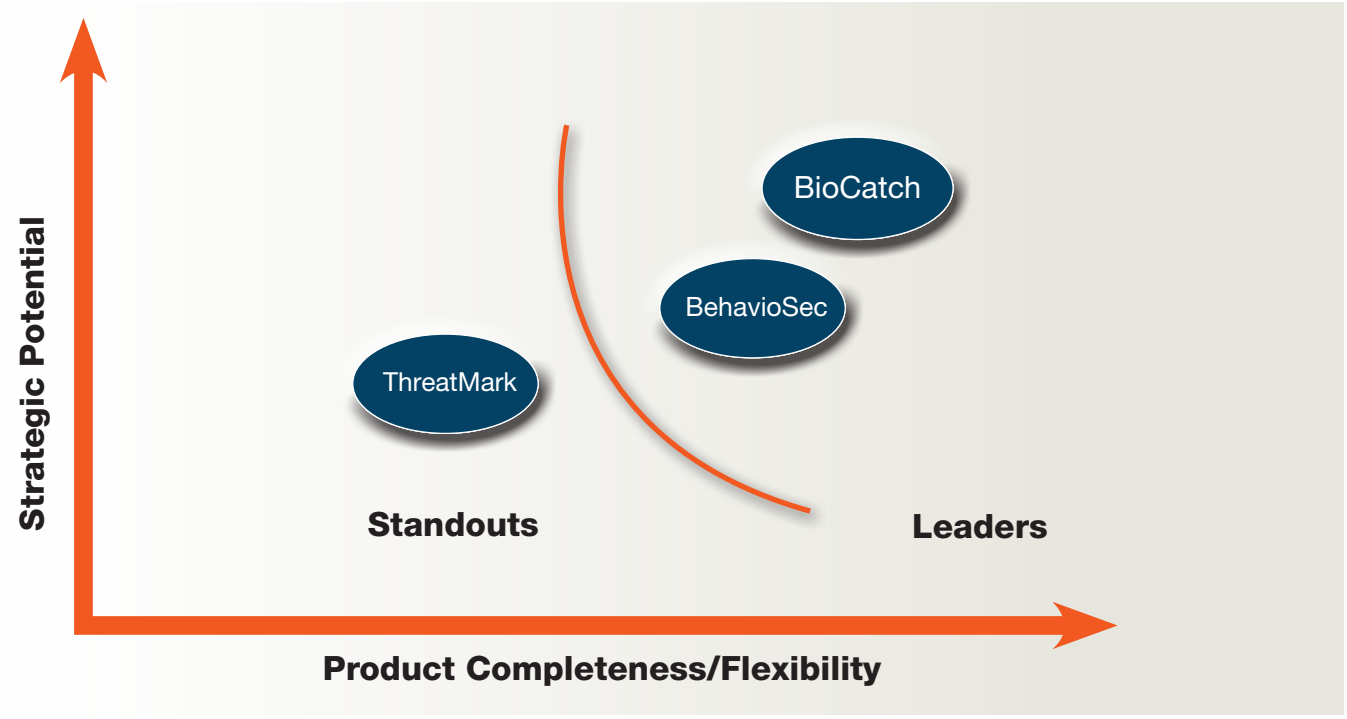
Prove (formerly Payfone) rebranded in early 2021 and, including the earlier acquisition of Early Warning Services, now serves 9 of the top 10 banks in the US, covering billions of calls every year. Prove has carrier and mobile network operator partnerships in the US, Canada and UK, enabling them to leverage the carriers own device authentication to verify possession and identify SIM swaps. Prove solution can be used for identity proofing (confirming the owner of a phone for onboarding), authentication and fraud detection. Proves broader offering includes unique device based behavioral analytics that maintains continuous knowledge of device possession (even when not in use) from their acquisition of UnifyID in June 2021 and push-based multi-factor authentication providing a comprehensive solution for mobile-first organizations.

Smartnumbers

Smartnumbers UK heritage has meant overcoming some tough privacy regulation challenges whilst still helping their large enterprise customers mitigate significant fraud volumes and reduce customer authentication effort. They are the default provider for the UK's largest banks. While taking advantage of their privileged network access in the UK, their Protect solution can also be deployed in a carrier agnostic fashion, allowing for quick implementation globally. Their case management capability will enable analysts to manage the fraud investigation process efficiently, and their industry-standard models further contribute to getting customers up and running quickly. They operate exclusively through partners, notably BT and Nuance, which gives them plenty of strategic promise to expand beyond their traditional markets.

Behavioral Biometrics

Figure 7: 2022 Intelliview Map - Behavioral Biometrics



Leaders (listed in alphabetical order)

Each participant in the Behavioral Biometric category is graded base on the completeness of its core offering as well as its demonstrated ability to integrate with a company's existing authentication and fraud prevention initiatives. As an emerging technology, behavioral biometrics do not yet comprise a single, complete solution to authentication or fraud prevention efforts and will always be part of a larger solution that encompasses enrollment, returning a confidence score when called upon to authenticate a known individual and alerting companies when certain behavioral traits indicate that an individual is highly likely to be an imposter.

BehavioSec

Founded in 2008 and considered the pioneer of the behavioral biometrics category, BehavioSec has grown its set of capabilities organically in response to demand for transparent mechanisms to augment outdated and vulnerable authentication methods like SMS-based 'one-time-passwords' (OTPs) and knowledge-based questions while also accelerating their demise by providing a viable and sustainable replacement. BehavioSec core technologies use cadence, touch screen interactions, and mouse/trackpad movements to evaluate whether input comes from the expected user or a fraudster. The "signals" their analytic engines detect are then used as inputs into a broader risk engine, ID platform or third-party tools. Of special note, their solution's detection of IP change, origination from a new country and location overlap augment solutions from providers of Network Intelligence and Authentication.

BioCatch

BioCatch claims exclusive focus on Behavioral Biometrics with primary focus on fraud detection. No authentication. They are distinguished by a long track record and deep focus on the workflows of "fraud operators." They monitor the broadest array of physical and cognitive indicators (claiming 2,000) and patents (60). They are also distinguished by their understanding of the processes that simplify the tasks of Fraud personnel. For instance, it allows fraud operators to define and propose new rules as they arise and defines a 7-day period for them to be provisional and then a mechanism for a "user with relevant permission" to approve it.

Standouts

ThreatMark

A respondent that makes it hard to distinguish between Network Intelligence and Behavioral Biometrics. Its scoring is based on "Device Reputation" is built on "extensive device fingerprinting". Yet ThreatMark also claims to perform with a significant amount of behavioral profiling and, indeed, believes that "the most reliable and efficient way to detect SIM-swapping is by behavioral profiling" because fraudsters can't replicate the behavior biometrics of the legitimate user. Based on constant monitoring in the background ThreatMark is able to provide risk scores based on real time monitoring of behaviors which are to a central Analytics server, which applies ML and "AI" to render a score in real time.

Intelligent Solutions for the Low Effort Authentication and Fraud Detection

Businesses are coming to grips with permanent changes in how their employees and customers work, shop and seek assistance. Large percentages of employees, including contact center agents, want to remain working at home… at least part of the time. Customers continue to want to shop or seek assistance at nearby banks or storefronts, even as their online and smartphone-based activities crescendo. Security professionals are forced to treat each new contact like a first encounter. Making the most of the information available to determine who to trust and what they can accomplish.

In 2022, the watch phrase will be to "do more with less." Don't ask pointless questions. Don't rely on passwords. Don't make customers do the work. Instead, work in the background using physical and behavioral characteristics (biometrics) and "metadata" generated in the course of the interaction to increase confidence that that the user is who they claim to be. The firms and technologies under review in this document are perfectly suited to assist enterprises as they build strategies for secure and trusted conversational commerce.

.

Nuance

Headquarters: Burlington, MA
Year business started: 1992
Investment/Funding: N/A
Revenue: 2020 Revenue: ~$1.5B
Number of employees: Approximately 7,100 employees total.

CAPABILITIES

Technology - Voice Biometrics

Core Authentication
Nuance's voice biometrics engine uses state-of-the-art deep neural networks to authenticate a person with as little as 0.5 seconds of audio and achieve up to 99% authentication success rates. The system authenticates legitimate customers and detects known fraudsters by comparing input voice audio to a collection of stored voice samples ("voiceprints") that are known to be authentic or fraudulent. Voiceprints can be enrolled with as little as 5 seconds of audio. Nuance's voice biometrics engine is protected against voice morphing, adaptive text-to-speech, and other forms of audio spoofing. It supports both text-independent (passive) and text-dependent (active) voice authentication, including text-independent voice authentication in the IVR and contact center. And it can accurately authenticate a person through background noise, illnesses, face masks, and other factors that somehow modulate the sound of a person's voice.

Text Dependent: A text-dependent voice biometrics implementation prompts a person to repeat a specific vocal passphrase that matches the phrase they recorded when they enrolled their voiceprint. Nuance's voice biometrics engine virtually eliminates the need for text-dependent verification due to its extremely high accuracy and low audio requirements for short-utterance text-independent verification.

Text Independent: A text-independent voice biometrics implementation works continuously in the background to verify a person from their natural speech as interact with a human or virtual agent such as a speech-enabled IVR. Nuance's latest enhancements to our voice biometrics engine achieve sufficient performance to empower organizations to authenticate customers and employees with extremely short utterances in any context.

Minimum Authentication Net Speech Requirement: 0.5 seconds
Minimum Enrollment Net Speech Requirement: 5 seconds

Fraud Detection
Watchlist: Nuance does not limit fraudster watchlist sizes, instead offering individual customers personalized support and guidance based on their unique situations. That said, our financial services customers generally maintain watchlists in the hundreds to thousands range.

Cross matching
Nuance Gatekeeper includes audio clustering tools for detecting fraudsters via cross-matching. **Clustering analysis** groups similar audio samples together based on shared biometric characteristics of the speakers within. Clustering enables fraud teams to identify previously unknown fraudsters, for example by uncovering where a single caller is trying to access different customer accounts. Once a suspicious person is identified, a voiceprint can be created from the audio samples and then added to the fraudster watchlist. Fraud teams can then run **backwards searches** to detect where that fraudster appears in other historical call logs, gaining valuable data to build their case against the fraudster and obtain a clearer picture of total exposure. Through our state-of-the-art voice biometrics engine, Nuance's tools enable fraud analysts to perform efficient clustering at scale.

Describe a typical workflow
As a person calls into a contact center or IVR, the Gatekeeper Risk Engine determines if the caller is fraudulent in real-time, based on a combination of biometrics comparisons (authentication, fraud watchlist detection), other risk factors and risk associated with previous engagements in the journey. If Gatekeeper determines the call to be of high risk a fraud alert is triggered in real-time (while the call is live), which can be made visible to the call center agent and the Gatekeeper Web Portal, where fraud analysts manage and review fraud cases. Due to Gatekeeper's ability to generate fraud alerts in real-time, fraud alerts can also be used to trigger business logic that would, for instance, transfer the live call to a fraud specialist queue trained to handle fraud events. Call center agents are also able to manually trigger alerts in Gatekeeper if they have reason to suspect the call as being fraudulent per their business processes. These alerts would also appear to fraud analysts in the Gatekeeper

Web Portal. The Gatekeeper Web Portal is the fraud analyst's window into fraudulent activity in the IVR, call center, or digital channels. The fraud analyst can review high-risk engagements and begin to investigate them individually. A fraud manager can assign individual engagements to different fraud analysts for review. Within each engagement, a fraud analyst has access to all the details of what generated the alert (biometric scores, the Gatekeeper Risk Engine decisions, as well as accompanying metadata). They can also listen to various recordings associated with a given engagement to help conclude whether this was indeed an attempted fraud attack. Fraud analysts can also complement their investigations using Gatekeeper with information and data coming from other systems at their disposal (e.g. internal account management systems).

Presentation Attack Detection Capabilities
Nuance Gatekeeper thwarts presentation attacks by using two types of AI-based playback detection to test whether an audio sample represents live speech or a recording that impersonates an authorized speaker. **Channel playback detection** detects the presence of signal artifacts introduced by the recording and playback process, and isolates playback attacks based on a user-defined false alarm rate. **Footprint playback detection** determines if two audio buffers correspond to the same utterance. The system compares the current audio with a saved "footprint" of a previously collected authentication passphrase. If the two footprints match too closely, the current one is marked as a recording.

Synthetic Speech Detection Capabilities
Nuance uses AI to guard against synthetic speech by detecting telltale signs of voice recordings and artifacts created during voice morphing, adaptive text-to-speech, and high-quality text-to-speech synthesis.

Approach to tuning, calibration, and optimization of end-user implementations
Gatekeeper voice biometrics technology is used as part of the Risk Engine decision-making. The built-in models for voice biometrics can provide highly accurate performance for most standard contact center, IVR, and digital applications. Gatekeeper also features capabilities to allow for online improvements to performance automatically or with minimal intervention. For instance, the system improves voice biometrics performance through voiceprint adaptation (profiles are automatically updated as more data becomes available). Users of the system can also adjust Gatekeeper parameters to refine performance in accordance with business objectives. This is done with the insights provided by the Gatekeeper reporting portal. Gatekeeper models, whether for voice biometrics or the Risk Engine, can be further updated using data from a specific customer's environment. This allows for further performance improvements as the system learns the specific environment's characteristics more deeply (e.g. telephony, platform technologies, caller population). Tuning can be performed seamlessly in the background without disruption to a live system.

Agent User Interface
An out-of-the-box agent console is provided with Gatekeeper. This can be used standalone or integrated into any current agent desktop as a web widget. Alternatively, an Agent REST API is provided to allow a client to develop their own agent desktop.

Management Reporting and User Interface
Gatekeeper is performed via a web user interface. If an organization uses Active Directory Single Sign-on, this can be configured for access to the Gatekeeper web interface, preventing the need for additional usernames and passwords. This is true for both the Microsoft Azure hosted Gatekeeper solution and the on-premises solution. Nuance Gatekeeper's Caller ID Validation capability is designed and implemented to allow extensibility whereby we ingest all factors provided by our partners, including device- and number-based, along with factors we generate, to provide a holistic risk assessment for a given call or interaction. Nuance partners with Neustar and Smartnumbers, serving the North American and European markets.

Call Anomaly Detection
The combination of call validation, device print, and conversational biometrics capabilities work together to recognize anomalous behavior from the point of origin (device) through the carrier network and post answer integration—be it with a live person or with a simulated actor such as a bot or synthesized speech.

Detection Capabilities
Network validation provides pre-call outcomes, guaranteeing that calls are placed from devices that own the ANI specified, and when not, assessing the likelihood of spoofing. These factors are combined with all other indictors available to the Gatekeeper Risk Engine when making an authentication assessment.

Behavioral Biometrics
(Partner with BehavioSec)

Decision Making Approach
Underlying the Gatekeeper platform is an AI Risk Engine that uses state-of-the-art deep neural networks to synthesize the data output of biometric and non-biometric factors, plus other available data such as engagement and authentication history. The Risk Engine then returns a decision (authentic, fraud) and an overall risk score for a given session or interaction and across engagement journeys. Clients can retrieve the results of each individual feature or the aggregated result programmatically during a session.

Integration
The Gatekeeper platform is built to support flexible integration with customer systems depending on their unique environment and business requirements. Gatekeeper supports integration with all major contact center platforms, including both Contact Center as a Service (CCaaS) and traditional on-premises telephony systems. Gatekeeper also provides APIs for its core functions as well as an SDK for mobile applications.

Authentication and Fraud Detection Methods
All the authentication and fraud detection methods listed here are offered as out-of-the-box capabilities of the Gatekeeper platform. Holistic risk assessments, voice biometrics-based and conversational biometrics-based methods and the fraud data share program are in-house capabilities developed by Nuance, while behavioral biometrics and network authentication are delivered via OEM partnerships with third party technology vendors BehavioSec and Neustar, respectively.

- **Holistic risk assessments** through the Gatekeeper Risk Engine based on deep neural networks that synthesize biometric and non-biometric factors, plus engagement history and relevant available third-party data to authenticate legitimate persons and detect fraudsters no matter the identity or device they hide behind.
- **Voice biometrics** verify legitimate persons and identify fraudsters in real time and post-engagement based on their unique voice signature. Real-time voice authentication compares a person's voice in the contact center, IVR, or a digital channel to libraries of known customer and fraudster voices. Post-engagement voice watchlist comparison compares historical call recordings and digital authentication attempts against a fraudster watchlist. Data mining, clustering, and backwards search capabilities enable fraud analysts to identify previously unknown fraudsters and then uncover where they appear in historical data.
- **Behavioral biometrics** authenticate legitimate users and identify fraudulent activity in digital channels by answering three questions for every session: Is this a human? Is this a good human? Is this the right human? The system continuously monitors user behavior and device signals to verify known or trusted users while identifying suspicious behavior, anomalies, and session changes to detect bots, remote access trojans, new account fraud, and other forms of fraud in digital channels.
- **Conversational biometrics** verify users and prevent fraud in messaging and voice channels by detecting suspicious signals in typed or transcribed text in real-time and through post-engagement analysis. In this way, it is the only biometric modality that can passively authenticate users in both digital and voice contexts. Conversational biometrics prevent hard-to-detect forms of fraud such as social engineering of live assist or contact center agents and fraud mules hired to read from scripts.
- **Network authentication** inspects calls from within the network and compares caller IDs against a watchlist of known compromised ANIs to authenticate trusted calls and detect ANI spoofing, virtualized calls, and other threats even before they reach the IVR or contact center.
- **A fraud data share program** curated by the Nuance Fraud Nexus Team enables anti-fraud teams to detect fraudsters the first time they ever attack the organization by drawing on fraudster voiceprints and metadata shared by their peers around the world.

End User Engagement

- Delivery Model: Direct model is primary by value of sales
- Partners: Neustar (call/network validation, North America); BehavioSec (behavioral biometrics, global); Smartnumbers (call/network validation, United Kingdom/Ireland)
  Channel partners: Nuance partners with numerous channel partners around the world, including contact center vendors such as Genesys, Avaya, Cisco and Five9; Microsoft, our strategic cloud partner; global SIs including Accenture and Deloitte; telco partners including AT&T and British Telecom; regional partners; and others
- Gatekeeper is a cloud-native solution that can be run in a hosted cloud environment as SaaS, in private clouds and on-premises, and on-device through an edge model. Gatekeeper can be purchased as a full platform solution or customers can license the core voice biometrics engine APIs to enhance their own applications.
- Pricing: Tiered pricing, based on volume, per transaction – this allows price to adapt to different sizes and volumes of deployments
- Nuance has approximately 1,600 R&D employees and 2,350 issued patents (as of 9/2020).

Vision & Plan
Nuance's vision is of a truly passwordless future, where all businesses, large and small, leverage affordable inherence and ownership-based systems, providing a pleasant and efficient user experience that quickly authenticates legitimate users while provide strong fraud protection across every interaction channel.

Over the coming years, the intelligent authentication market will consolidate onto a few main providers in each geography, further broken down into a smaller subset of providers who operate across regions. Both the consumer- and corporate-facing Identity & Access Management (CIAM and IAM) markets will move away from device-centric identity towards voice and behavioral biometrics as the primary modalities that consumers bring with them across devices and channels. Fraud prevention teams will continue to take a "swiss cheese" approach, bringing on intelligent solutions that layer biometric and non-

biometric factors with AI for real-time prevention and detection, and utilizing biometric analysis tools as a key component of their fraud investigation workflows.

Meanwhile, Nuance will empower fraud teams with a unified solution that stops fraud across channels by detecting human and non-human attackers based on intelligent, contextual risk assessments with biometrics at the core. Nuance will also become a central figure bringing together fraud teams from around the world to join forces in the global fight against fraud through a rich data-sharing consortium and a range of events and thought leadership.

Key Differentiators:

- Nuance Gatekeeper is the only solution that delivers integrated biometric authentication and fraud prevention in every voice and digital channel, enabling organizations to streamline and protect their entire customer journey through a unified platform.
- Nuance Gatekeeper delivers the fastest and most accurate authentication and fraud prevention performance in the world, capable of verifying a person with as little as half a second of audio; capable of achieving 99% authentication success rates; and capable of detecting 90% of fraud with high accuracy.
- Nuance has a proven track record of successful authentication and fraud prevention deployments around the world with customers who report better ROIs, higher fraud loss savings, and higher authentication success rates than organizations deploying competing solutions.

About SymNex Consulting

SymNex Consulting works with some of the most innovative and customer centric organisations to help them make the case for, design and implement transformational changes to the telephone welcome experience. Delivering dramatic improvements in the efficiency, security and convenience of these process through technology, pragmatism and behavioural understanding.

About Opus Research

Opus Research is a research-based advisory firm providing critical insight and analysis of enterprise implementations of software and services that support multimodal customer care and employee mobility strategies. Opus Research calls this market "Conversational Commerce" with tailored coverage and sector analysis that includes: Self-Service & Assisted Self-Service, Voice & Call Processing, Web Services, Personal Virtual Assistance, Mobile Search and Commerce and Voice Biometrics.

For sales inquires please e-mail info@opusresearch.net or call +1(415) 904-7666