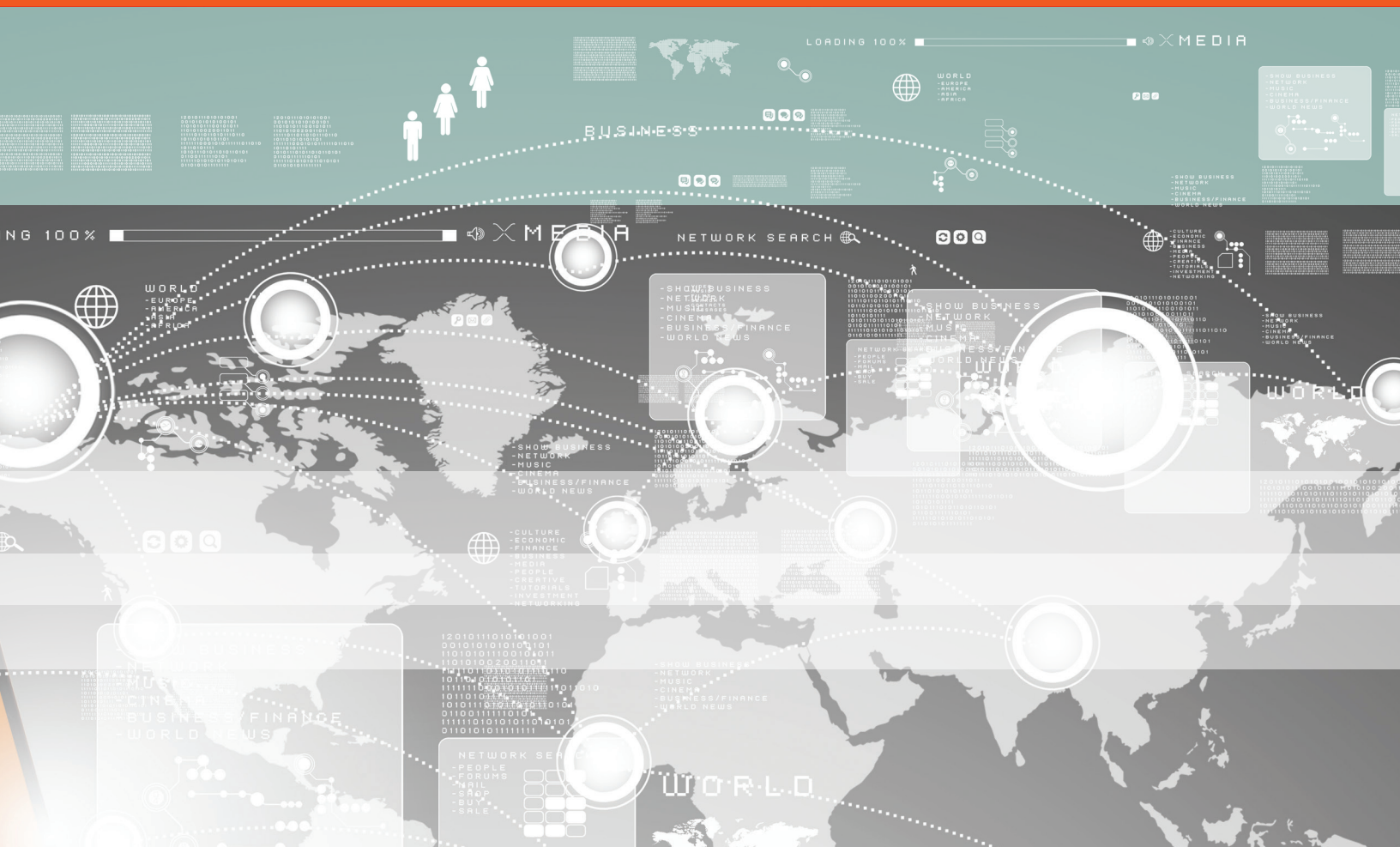
2022 Intelligent Authentication and Fraud Prevention Intelliview

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.

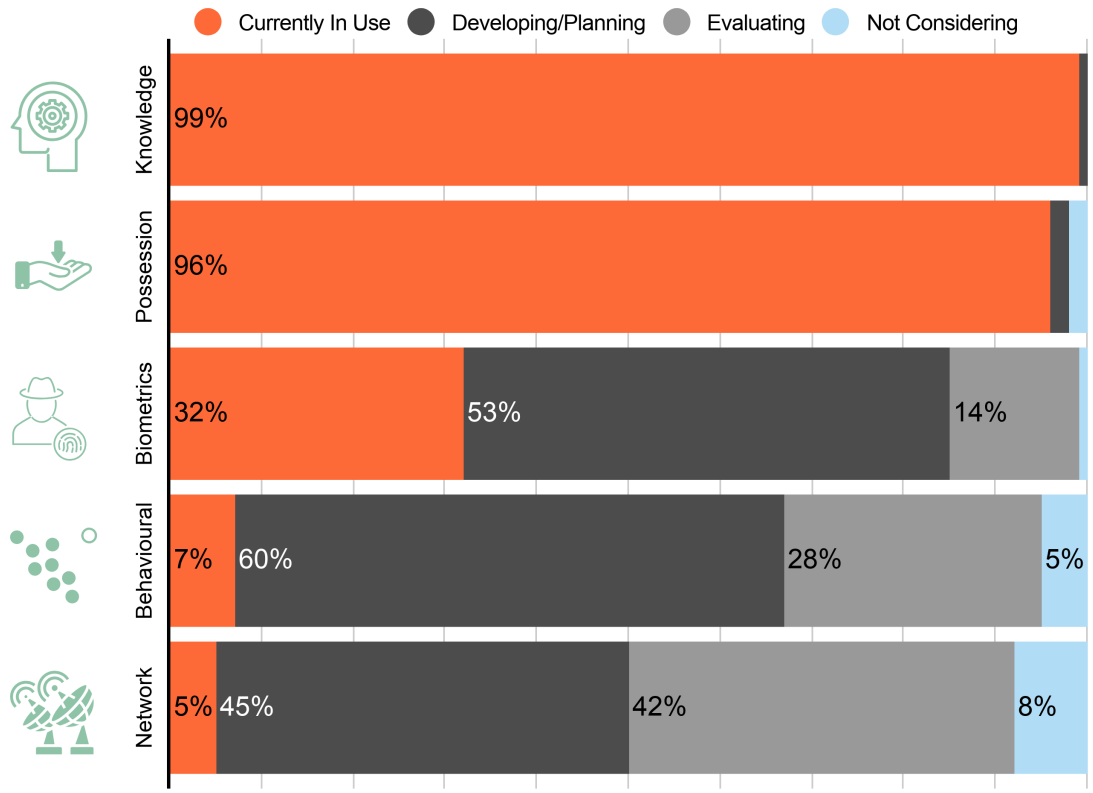
Field Results Show Growing Interest in New Authentication Methods

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

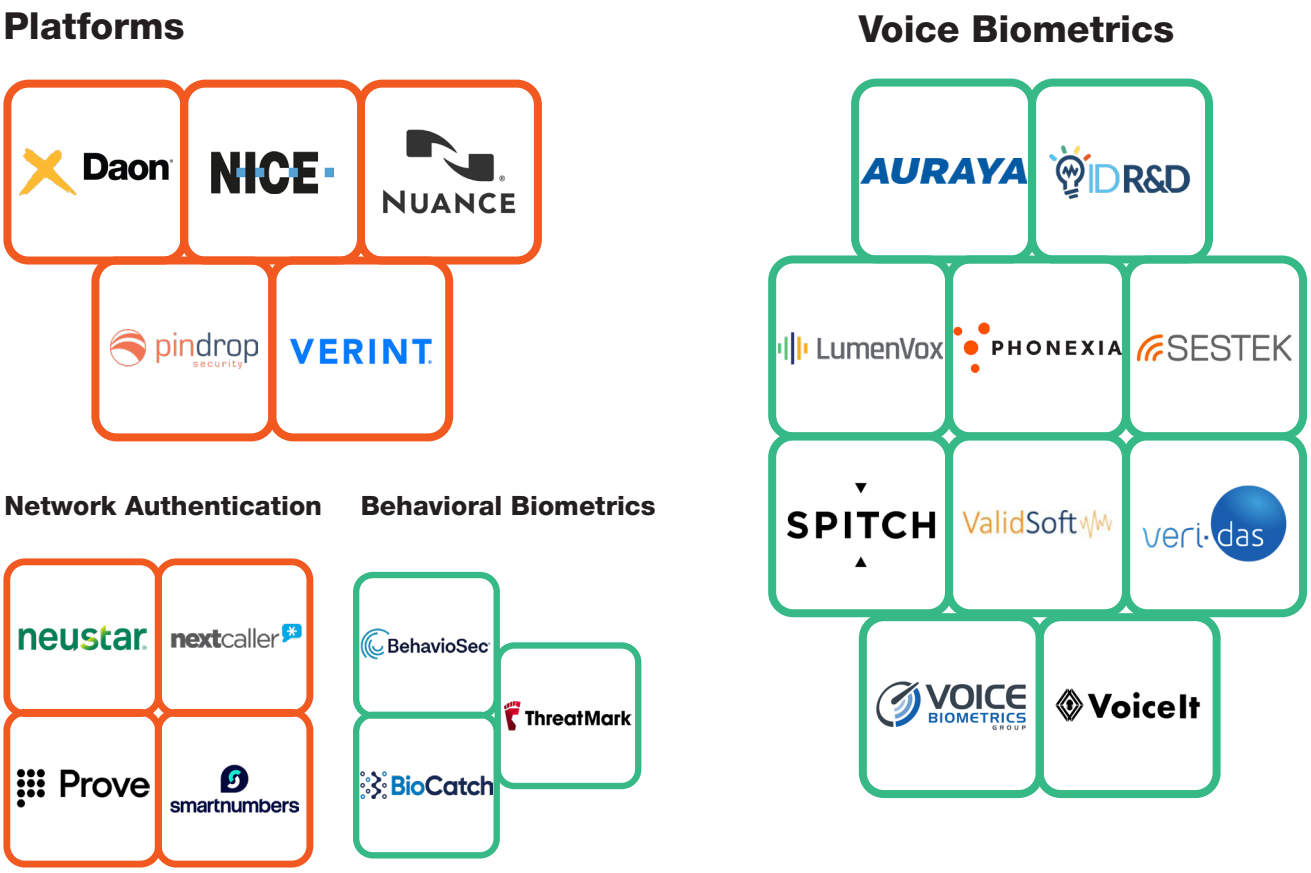


Firms Included in the Intelliview

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.

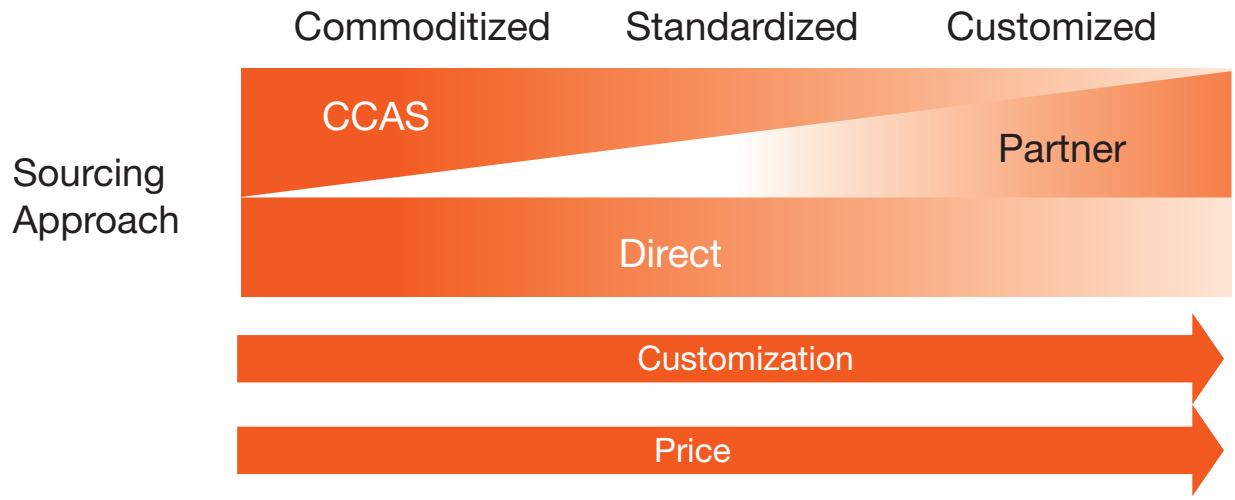
Many organizations that lifted and dropped their existing knowledge-based authentication processes onto these platforms are now beginning to look at more modern security approaches such as voice biometrics. These are now significantly more accessible as a result of the standardized integrations on these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

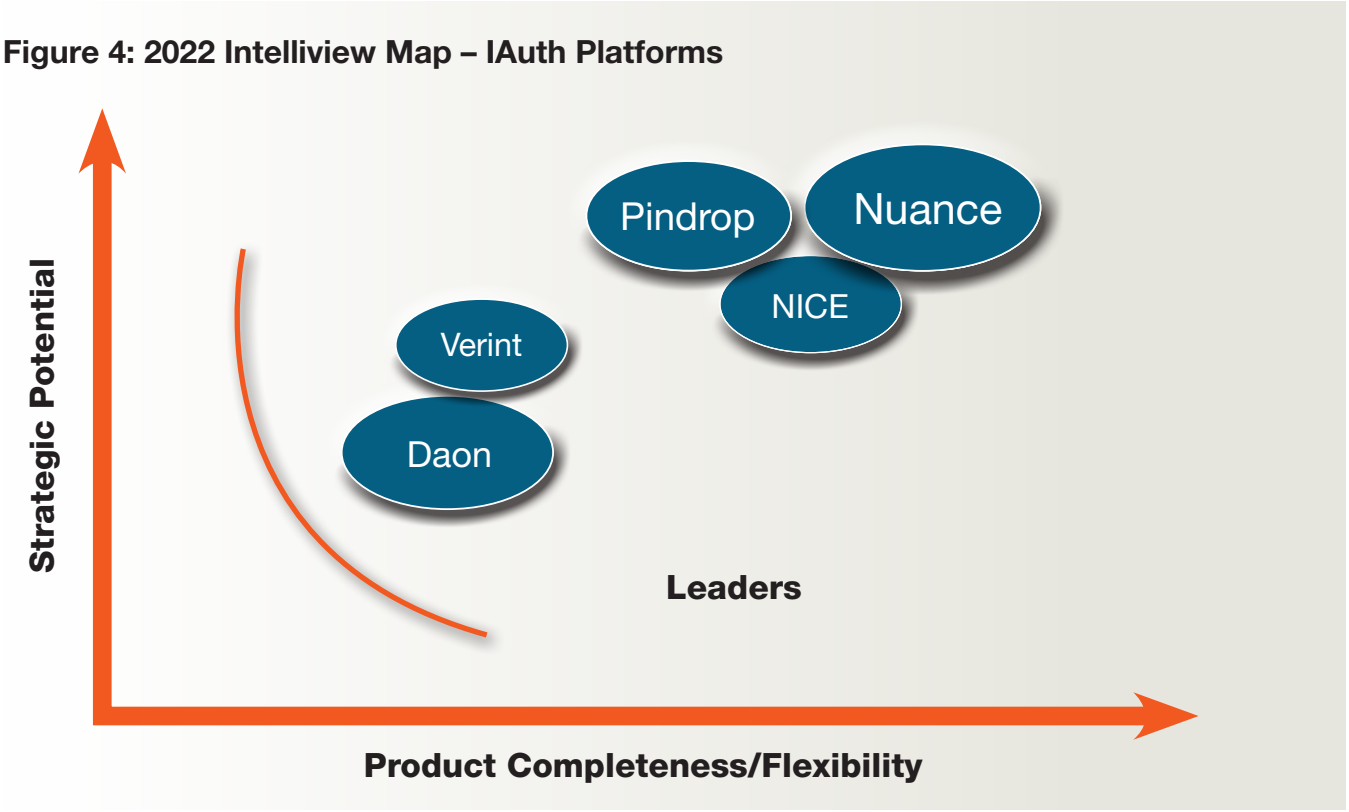
- **Product Completeness/Flexibility** – captures how current product capabilities meet real customer requirements as evidenced by referenced implementations. It includes an assessment of flexibility to adapt to specific needs as demonstrated by reference customers. Platform providers receive the highest 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

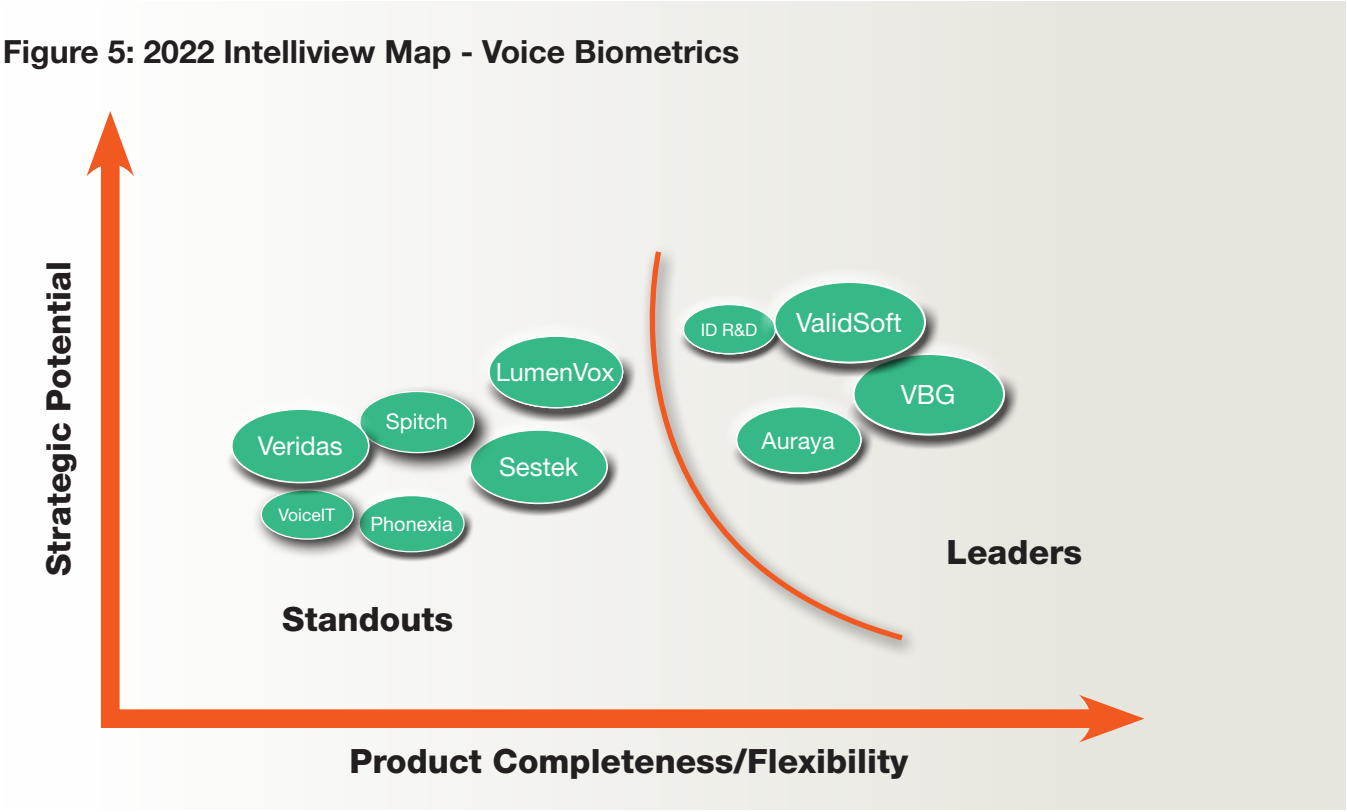
Pindrop's historical focus on fraud prevention continues with best-in-class analyst experience and new tools to predict which accounts are most at risk in advance of any loss. Their phoneprinting technology and consortium data now covers almost 5 billion calls and 2 million fraud events. Their passport 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.

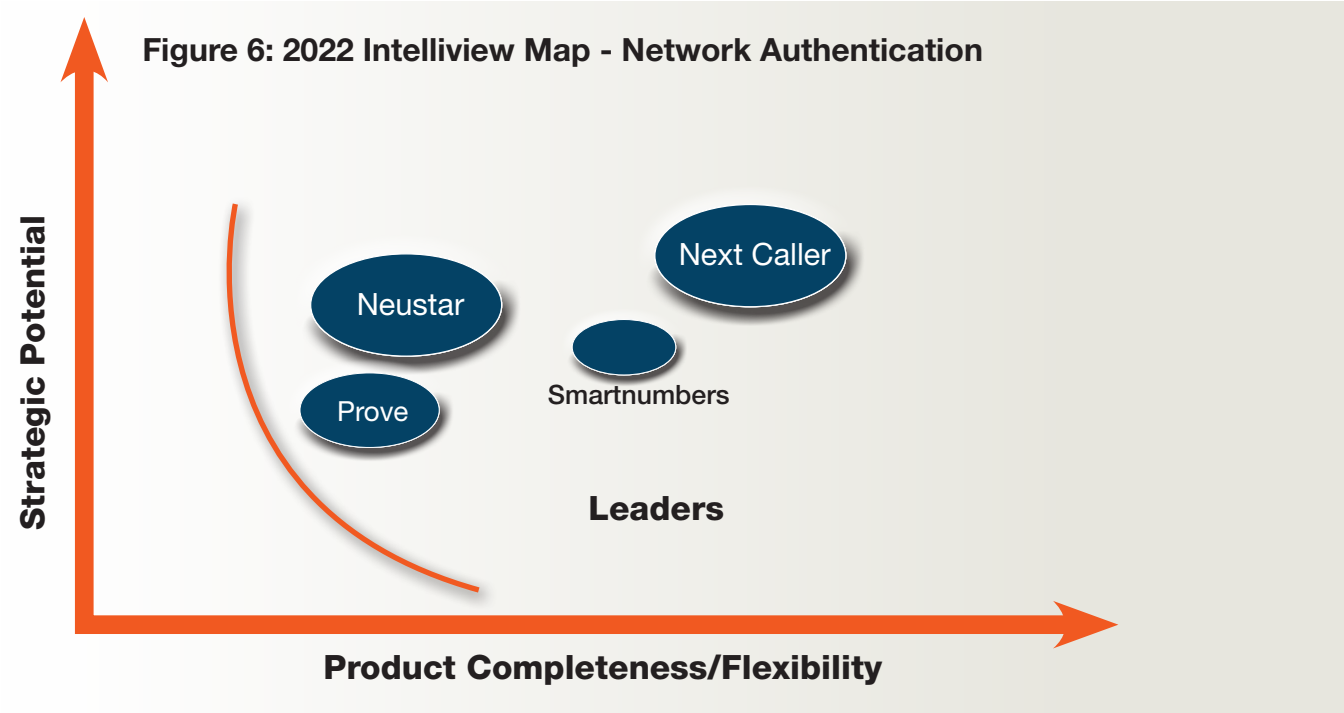
Google

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

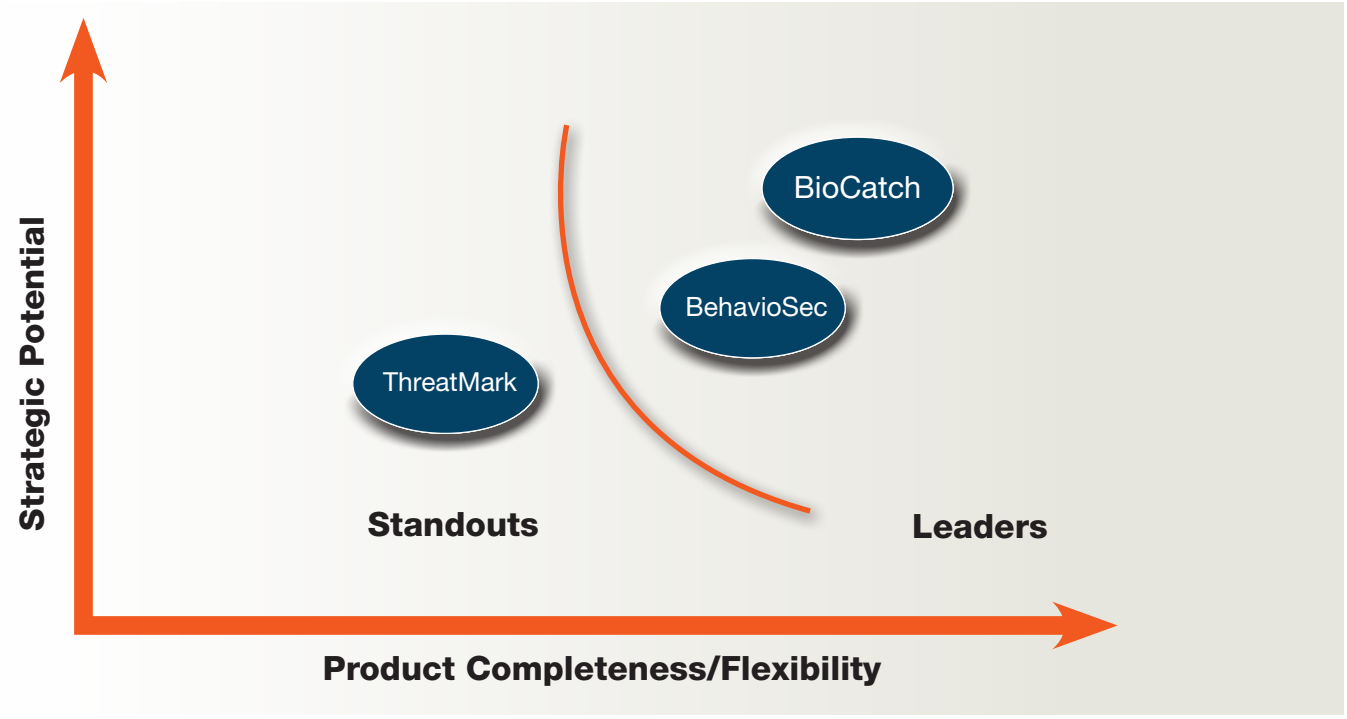
Prove (formerly Payfone) rebranded in early 2021 and, including the earlier acquisition of Early Warning Services, now serves 9 of the top 10 banks in the US, covering billions of calls every year. Prove has carrier and mobile network operator partnerships in the US, Canada and UK, enabling them to leverage 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.

Appendix A - Company Dossiers

Auraya Inc.

Headquarters: Delaware USA; NSW, Australia
Year business started: 2009
Investment/Funding: GERP (owned by ICM Group
Revenue: N/A
Number of employees: 16

CAPABILITIES

TECHNOLOGY – VOICE BIOMETRICS

Core Authentication
Text Dependent: Auraya's voice biometric technology utilizes its AI-powered core voice biometric engine ArmorVox™. ArmorVox has processed hundreds of millions of voice biometric transactions over the last decade using increasingly sophisticated machine learning algorithms to deliver best in-class voice biometric performance. ArmorVox's patented speaker-specific background models, automated threshold settings and active learning algorithms deliver a user selectable false-accept rate for each transaction on every voiceprint. ArmorVox, with its fused speech recognition and speaker verification capability, enables any required phrase to be checked for accuracy as well as verifying the identity of the voice. The patented speaker specific background models and automated tuning enable any spoken language to be used to enroll and verify speakers.

Text Independent: For text-independent use cases ArmorVox offers both digit-independent and text-independent options. Digit-independent provides an option which increases security performance with less audio when people say digits. Digit-independent increases usability for BOT transactions where a speaker can simply provide a series of digits such as ticket number and card number and be identified and verified in the same utterance.

Short Utterance Text Independent Authentication: ArmorVox requires a minimum of 2 seconds of net audio to begin authentication. Each 2 second segment of speech is aggregated and analyzed with a typical ~95% pass at one in 1000 FAR with 6 seconds of net speech when using text dependent unique phrase. This performance assumes approximately one minute of audio for enrolment and active learning processes to optimize voiceprint performance.

Minimum Enrollment Net Speech Requirement: Auraya recommends enrolling a minimum of 24 seconds of net speech for a text-independent voiceprint. Whilst less voice can be used this may result in higher levels of false reject. Additional voice can be automatically added to the voiceprint using active learning when more authenticated voice is available.

Fraud Detection
Watchlists: Can be as long as required to suit the use case. Auraya's EVA Forensics solution has unlimited numbers of lists with unlimited number of voiceprints per list. Typically, the default setting for any lookup list is set at 100 individual voiceprints. This default setting can be changed to be any number that is needed for the use case scenario. ArmorVox uses its unique AI known as anti-models, to distinguish between 'near neighbors' on a lookup list.

Crossmatching: ArmorVox carries out >150million crossmatches per hour on a single server. Adding additional servers (CPUs) increases the number of crossmatches able to be completed within a given time frame. Auraya's proprietary methodology for scaling of the fast-crossmatching process utilizing AI, means any sized crossmatching process is achievable. EVA Forensics uses auto scaling capability on the audio preprocessing and biometric matching which enables analysis on a large scale to be performed.

Describe a typical workflow: EVA Forensics has a powerful set of capabilities useful to organizations and forensics analysts looking to manage fraud and find identities in live conversations with agents and bots as well as detecting matches in historical recordings. EVA Forensics is used to detect fraudulent activity in customer onboarding processes on websites and apps. The customer is simply prompted to click on a link and say the digits displayed to create a voiceprint. The audio from the enrolment is then compared against other new customers or recently onboarded customers voiceprints. Typically, organizations will load recordings of identities into list(s) using EVA's orchestration tools.

Presentation Attack Detection Capabilities
EVA uses ArmorVox AI to create a layered approach to detect and defeat presentation attacks. The first layer in the defense process is device identification. EVA checks the device ID (CLI, IP address, encrypted keys, etc.) and defines the level of trust associated with the device being used to collect a voice sample. EVA integrates information about devices and transaction risk from other risk systems, to inform and modify settings to adjust processes and biometric sensitivities based on risk profiles.

Synthetic Speech Detection Capabilities
EVA uses the 'model' function within ArmorVox to compare audio to the models of synthetic voice samples. Where voiceprint has been created using a synthetic voice generator, the artifacts of the synthetic voice generator are used to flag the audio as 'synthetic' so even if the voice scores well against the candidate, the verification attempt will fail as it sounds too similar to a synthetic voice model.

Results of Recent Benchmarks
ArmorVox has been benchmarked in production systems by one of the largest telecommunication carriers and one of the largest contact center operators in the world. In both of these comparisons ArmorVox's performance was directly compared against the incumbent voice biometric performance. This real-world benchmark using production data provides the best comparison along with higher degree of accuracy in performance, as opposed to laboratory experiments conducted using artificially created or pre-configured data sets. Anonymized results from these benchmark tests are available under NDA to organizations that are considering adopting Auraya's technology.

Approach to Tuning, Calibration and Optimization of End-User Implementations
Auraya recommends an optimization process using a `supervised learning process' is carried out for each implementation when the system is initially deployed. This optimization process uses the client's own data on their system. Importantly, no data ever leaves the clients secure environment, and no external data is imported into the clients controlled and secure environment. This system optimization supervised learning process involves using production data from the initial five thousand enrollees. This process usually takes less than half a day and can be carried out without interrupting the production system.

Agent User Interface
EVA's Agent User Interface has an extensive suite of controls and indicators that can be made available to Agents. The agent desktop can be configured so different agent skill groups have access to some or all of the Agent User Interface functionality. Auraya recommends that the general Agent pool use the minimum indicators and controls to ensure simplicity in agent training and clarity of process for all calls received. Specialist agents can be provided with additional controls and indicators such as "remove biometrics" and "update biometric print" due to changes in a voice caused by injury etc.

The controls available include claimed IdentitY; active verification status; passive verification status; potential fraudster status; enrolled but not yet verified status; enabling an enrolment activation; confirmation of authentication of claimed identity prior to enrolment; enabling a specific OPT IN process; enabling an active learning on a specific conversation; enabling opt out; deleting a stored voiceprint; confirmation of a single speaker in a conversation; and enroll a new voiceprint.

The Agent User Interface includes all required security protocols to ensure cyber resilience and interconnection using open standards like SAML to ensure log on for authorized agents is included within their single sign on process managed by the organizations Identity Access Management system such as PingFederate, OKTA, Auth0 and others. These same IAM systems set the controls that are visible or usable to be on a least privilege basis.

Auraya has a long history of endorsing and using open APIs to interconnect with other systems. The EVA solution templates can be modified by the client or their service providers to deliver a customized solution meeting the specific needs of the enterprise. In this manner the standard Agent User Interface can be adopted as a pop up on any agent screen or alternatively the open APIs can be used to incorporate the required controls and indicators into any preferred agent operating system such as Salesforce, Zendesk, Service Now, Twilio, Bright Pattern, Five9, Genesys and others.

Management Reporting and User Interface
EVA's Management Console has an extensive suite of capabilities for system analysts and administrators to use to control the enterprise voice biometric solution and produce both real-time and historical reports. The Management Console can be used to configure EVA setup and enable configurable options as well as enabling system optimization and biometric performance auditing.

EVA's Management Console contains a full suite of forensics analysis tools enabling any system audio to be listened to by an analyst, curated by removing silence and non-voice artifacts and examined using a spectrum analysis tool. The audio can be compared to other voiceprints and additional audio can be added using an active learning process.

Auraya's philosophy with respect to reporting is to enable organizations to incorporate voice biometric system data into their existing enterprise and contact center specific reporting platforms. Most organizations prefer to add the required voice biometric information into existing systems so a coordinated and holistic approach to analyzing and reporting on all elements of a customer journey across all touchpoints is available for real-time and historical analysis. To this end, Auraya's standard approach is to configure EVA to provide all relevant real time and historical data to an S3 bucket or similar repository and use CloudWatch or other tools used by the organization to curate the data for the enterprise and contact center reporting systems.

EVA's Management Console contains a rich analysis tool set for fraud management and specific reporting for fraud analysis providing real-time and historical information in tables and graphs. All data created by EVA Fraud Manager is available for enterprise and contact center reporting systems, so a coordinated and holistic view of all customer interactions is available.

TECHNOLOGY – NETWORK AUTHENTICATION AND FRAUD DETECTION

Device/Number Possession
EVA utilizes device identification data such as IP address, CLI and other device identity information provided by identity and access management systems such as Ping Federate, Auth0 and OKTA from end points such as computers, laptops, tablets and smartphones.

SS7 Data Access
Vodafone and Telstra are Auraya Reseller partners that provide voice biometric solutions powered by ArmorVox that use network-based device ID and other metadata as part of the solution. Dubber, an Auraya Reseller partner, is licensed to use ArmorVox and EVA solution templates within its Voice Analytics functionality. Dubber's cloud-based call recording capability is integrated in AT&T, BT, Zoom, Cisco and other global carriers. Dubber incorporates network level device ID and other metadata to inform its voice biometric and fraud management capability.

Carrier Partnerships: Telstra Australia, Vodafone Global, and via Dubber, AT&T, BT, Zoom, Cisco and others in Global Markets. Our Cloud based contact center platform partners such as Twilio, five9's and Amazon Connect provide additional access to telephony platforms in all global markets.

Number/Device Ownership
Auraya interfaces with a number of Customer Identity and Access Management (CIAM) providers including OCTA, Auth0, PingFederate and other Cyber security and threat detection technology platforms to both inform the platforms of alerts from EVA and to inform EVA about threat levels that initiate step up security workflows including raising security thresholds on high risk transactions, adding random challenge questions for unknown devices or requiring passive verification of an entire call to detect bad actors. Carrier Reseller partners including Vodafone, Telstra and platform partners such as Five9's, Twilio, Amazon all provide inputs to this risk profiling and adaptation capability for the solutions that they deploy. Our Carrier level integrators such as Dubber have the capacity to manage their Device, SIM and PUK libraries and use this information to inform and react to their analytics and reporting processes.

Call Anomaly Detection
Auraya interfaces with a number of Cyber security and threat detection technology platforms to both inform the platforms of alerts from EVA and to inform EVA about threat levels that initiate step up security workflows in EVA's Fraud Management, EVA WEB and EVA Contact Center solutions, including raising security thresholds on high risk transactions, adding random challenge questions for unknown devices or requiring passive verification of an entire call to detect bad actors or lowering thresholds in hotlist matching processes.

Privacy Protection Mechanisms
EVA solutions enable end user Client organizations to retain and control all of their own data without any data ever needing to leave their secure on premise or cloud secure data stores. Organizations can configure EVA solutions to store data in different geographic locations so GDPR and other privacy legislation which mandates sovereign border protection protocols for PII data can be complied with. Importantly, no data needs to be provided to Auraya or any other third-party organization. Privacy protection therefore remains a client responsibility and capability to retain their data securely. EVA provides flexibility for client organizations to choose their preferred data encryption, retention and backup processes and procedures. EVA supports any commercially available database that an enterprise may choose to use. In line with regulatory requirements and good practice, all EVA solutions logically separate biometric data from PII data with an obfuscation table to match the data as needed for verification processes.

Available Integration Methods
ArmorVox, Auraya's core voice biometric engine can be supplied as a Java download or in serverless mode as Lambda or container. It can be run on any server or device or cloud service. EVA's solution templates are available in a number of downloadable services or SaaS and can be deployed on any server or cloud infrastructure. The most common way to deploy the EVA's solution templates is to use Cloud Formation to deploy a fully configured EVA solution in a secure client-controlled AWS instance. Once deployed the EVA solution template can be used 'as is' or customized to meet specific requirements. EVA Web uses any HTML5 compliant browser and needs no downloaded software on the device. If EVA Web functionality is required to be deployed within an app, an exemplar application code is provided to the application developer for incorporation into the target IOS or Android app.

Results of recent benchmarks
ArmorVox has been benchmarked in production systems by one of the largest Telecommunication Carriers in the world and one of the largest contact center operators in the world. In both of these comparisons ArmorVox's performance was directly compared against the incumbent voice biometric performance. This real-world benchmark using production data provides the best comparison along with higher degree of accuracy in performance, as opposed to laboratory experiments conducted using

artificially created or pre-configured data sets. Anonymized results from these benchmark tests are provided under NDA to organizations that are considering adoption of Auraya technology.

IMPLEMENTATION

Delivery Model: Auraya's delivery model is via an accredited specialist system integration reseller partner network and platform providers that incorporate our technology as part of their platform. Accredited partners are trained in all aspects of solution design and system implementation and ongoing support. *A*uraya also accredit end-user organizations that wish to establish an inhouse expertise. The inhouse team undertakes the same training and accreditation as reseller partners, in order to deploy and support their own systems. Auraya have a number of OEM partners that incorporate ArmorVox technology within their own platform so they can deliver an integrated solution which includes voice biometric enrolment, verification and identification process

Primary Partners: Accenture (global), Deloitte (global), PWC (NZ), ECS (UK Europe), Probe Group (Asia Pac), Connect Managed Service (UK), Dubber (Global), Telstra (Australia), Vodafone (Global), Fujitsu (Global), Unisys (Global), Acquire BPO (Australia & USA), Five9's (Global), Help Systems (USA Canada) and others.

Cloud-Based Services: Auraya technology supports Cloud based, On-premises and a hybrid, cloud and on premise. Auraya also provides its EVA Forensics as a SaaS service from multiple availability zones in multiple AWS regions. Auraya's technology is also provided as a managed service from a number of our partners (Vodafone, Telstra, Acquire BPO, Fujitsu and others)

Professional services are provided by our extensive network of Authorized Reseller partners (see above).

Pricing Model

- 'Enterprise' perpetual license fee
- 'Consumption-based license fee' based on a per enrollee per month basis with unlimited transactions with fee scaling based on the number of enrollees in the system.
- 'Consumption-based license fee' based on a per transaction with fees scaling based on committed volumes.
- 'SaaS' with the SaaS fee based on the consumption-based license fee.

IAuth intellectual property: Auraya has invested extensively in research and development for more than a decade bringing together a global team of experts in their field to develop unique systems, methods and core processes to create and continue to expand its core voice biometric technology and the applications that make it high performing, simple to deploy and support. Auraya has created an extensive patent portfolio consisting of six families of patents which cover core technology processes that deliver industry leading security, user convenience and deploy ability

Key Differentiators

- Voice biometric technology provides industry leading, consistent biometric security performance
- Flexibility in print type, channel and mode means all use cases for all channels use the same biometric engine and
- Open APIs and customizable solution templates speed the implementation process, allowing deployment in hours and days, not weeks and months.

BehavioSec, Inc.

Headquarters: San Francisco, CAUSA
Year business started: 2008
Year IAuth market contribution started: 2008
Investment/Funding: Venture-funded (Series B)
Revenue: N/A

CAPABILITIES

Technology - Network Authentication and Fraud Detection

BehavioSec performs device integrity checks including: a device is jailbroken; device is rooted; emulator is in use device is a common burner phone; an application shows evidence of tampering or cloning. BehavioSec further augments device analysis by performing checks against a global database of 1.5 billion devices and potentially raise a Risk flag and Risk score. The risk flag and risk score can then be used to detect suspicious activity or anomalies.

Technology - Behavioral Biometrics

User Authentication
Behaviosec helps protect the entire user journey which includes enrollment, account opening, login and in-session transactions by continually capturing user behavior and assessing risk in real-time. The solution focuses on user behavior as it pertains to their interaction either with an application via two physical mediums:

- The keyboard on a desktop, laptop, or workstation (includes mouse movements)
- The user's mobile device, meaning a mobile phone or tablet (both Android and iOS supported).
- Hundreds of unique user behavioral signals are captured from both mediums and used to create a unique user behavioral profile.
- The information from the user's behavioral profile is also corroborated with additional environmental (i.e. more generic behavioral information) about the nature of a session: e.g. IP address, device type, etc. BehavioSec refers to these as Risk Flags.

New Account Fraud: New Account Fraud module detect cases of "New Account Fraud" (NAF), also called "Account Opening Fraud". The Population Profiling feature generates profiling statistics against all users to help distinguish between a new genuine user and a fraudster.

Login and Continuous Authentication: BehavioSec platform automatically creates and updates user-specific behavioral profiles starting with the initial interaction with the application via either a physical keyboard on a desktop or laptop, and/or via a mobile device (iOS or Android). User behavior is continuously compared to the user- specific profile and provides matching scores to confirm the user's identity throughout the entirety of a session.

Risk flags: In addition to the New Account Fraud and Continuous Authentication features mentioned above, BehavioSec provides risk flags that detect anomalies and reduce fraud. One or more of the following flags may be indicated as part of the results:

- Advanced User: Advanced User indicates that the user is highly familiar with the page and computers.
- Automodel: Indicates that a behavior pattern that matches a model was detected during a transaction or session.
- Bot Detection: Checks input data for robotic behavior (e.g., too- uniform typing rhythm, latencies, jittery mouse movement etc.).
- Coaching Detection: User has probably been coached to perform a transaction. The user did not act according to their own will, they might have been threatened to do this transaction or been misled by a malicious authority.
- Data Corrupted: Errors were found in the received behavioral data such as, null values or otherwise broken formatting.
- Data Integrity: Inputted data matches the collected behavior. It also describes the specific events that caused it to trigger such as cut & paste, auto completion, password managers etc.
- Device Changed: Device (useragent string) has changed during the active session including if the device signature has significantly changed since a previous session.
- Device Integrity: Device shows suspect parameters.

- Device Reputation: Device used has a bad reputation.
- Duplicate Detection: Data contained has been duplicated by another user.
- IP Changed: IP address changed since the previous session and also provides a severity value, depending on usage frequency.
- Location Mismatch: Geolocation has been mocked or that IP-based and GPS data don't match.
- New Country: User is in the detected country for the first time.
- New Subprofile: New Subprofile was created for this profile.
- Numpad Usage Anomaly: User's numpad behavior was inconsistent during the session when compared to previous sessions (e.g., switching between numpad and numrow).
- One Hand Detection: User was likely to be typing with only one hand during a transaction or the whole session. This is likely to happen when the user is coached.
- Origin Hidden: Origin of the user has been hidden through methods such as VPN, TOR, etc.
- OTJS: Problem occurred while using One-time JavaScript (OTJS). It provides a description of the errors (e.g., the token expired, failure to decode, or the session or user ID does not match the one bound to the token).
- Page Definitions: Provide information about the different pages or screens where the user can enter data, so the behavioral engine knows what input to expect and what is optional. It flags if the input deviates from the expected.
- POC Usage Anomaly User's copy/paste behavior was inconsistent during the session when compared to previous sessions (e.g., pasting into fields where pasting wasn't used before).
- Rapid Location Change: Location of the current transaction or session is too far away from the last detected location for the given time span.
- Remote Access
- Remote Access indicates that one or more remote access protocols were detected in the session. If remote access is flagged, you can view a breakdown of software using the detected protocols by looking at the ratProtocol parameter.
- Replay Attack: Exact same behavioral data has been received in the past.
- Session Corrupted: Session level corruption (i.e., username changed during the session). A session ID cannot be shared between multiple users. If there are user IDs in sessionCorruptedUsers, then the session contains data from multiple users.
- Shared Device: Device has been seen during another user's session within the set time span.
- Shared IP: IP address has been seen during another user's session within the set time span.
- Tab Usage Anomaly: User's tabbing behavior was inconsistent during the session when compared to previous sessions (e.g., tabbing between fields).
- User Integrity: Calculates and displays the moving average of the scores and confidence values of the user. It flags if the Score or Confidence is too low, which may indicate a bad user profile.
- Whitelisted: User has been flagged as whitelisted by an administrator or third-party system. Note that this only indicates
- that the flag is set and does not affect how the system treats the user.

Device fingerprinting and IP detection
BehavioSec also checks for numerous “red flag” behaviors, such as: Hidden IP, VPN or TOR usage; Rapid geo-location change; Device switching; Shared device/ IP across accounts

Device Authentication
BehavioSec identifies the device and checks against a global database of devices for reputation and blacklisted devices. BehavioSec reports the type of device and its properties: model, display size, browser version, etc.

Fraud Detection
BehavioSec collects a wide range of behavioral data along with device information. The collected data consists of the following elements:

- All keyboards: typing cadence (speed, rhythm, intervals), mouse movements, touch screen pressure, motion, swipe length etc.
- Mobile devices: location, size and pressure of each click. Touchscreen gestures: motion size, pressure, speed, arc, etc. Orientation and movement of the device in 3D space.
- Device info: location, device type, platform, language, reputation, etc.
- All available signals are used as inputs to our machine learning engine in real-time to generate behavioral scores, risk scores, risk intelligent flags and identify threat vectors. These signals help detect fraudulent anomalies in real-time.

BehavioSec can be easily integrated with out of the box SDKs for iOS, Android and web-based applications. The SDKS enables the data collection - i.e., the end user’s behavior or interaction with the device or keyboard. In addition to the native SDKs, BehavioSec offers integration modules for frameworks such as Cordova and for platforms such as Nuance, ForgeRock, Ping Identity, etc. The SDK size ranges are approximately 34 KB for the JavaScript SDK, 240KB for the Android SDK, 2MB for iOS SDKs, depending on CPU architecture and standard frameworks included in the application.

Results of Recent Benchmarks
BehavioSec's customers have reported the following benchmark results:

- Accuracy: customers have reported accuracy rates of over 99% in confirming the identity of the user based exclusively on the behavioral data
- BehavioSec stops up to 99% of credential stuffing and other account take-over (ATO) attacks
- BehavioSec automates over 91% of false alarms and manual reviews
- Manual review / false positive review ratio is less than 1:1.

Approach to Scoring, Tuning and Calibration
The BehavioSec solution is packaged with ready-to-use modules which provide immediate value and are tuned over time by our machine learning engine. BehavioSec automatically detects new patterns across user sessions and provides the ability to customize and calibrate business rules. BOT and RAT and Fraud recognition are operational from the first day of implementation. After seeing several sessions from the same BOT/RAT, also new BOTs/RATs can be recognized even, if they have never seen before in the wild. ATO based on behavioral biometrics of individual users needs a trained profile from the customer, which is available after 2-3 sessions of the customer.

BehavioSec New Account Fraud (NAF) module consists of several built-in behavioral models which are compared against each users' input in real-time to detect Fraud. These models can be further fine-tuned and customized to make them more effective for the applications in use.

BehavioSec authentication module stores a specific user's behavior patterns and detects anomalies that may indicate fraud. These profiles are automatically refined with the machine learning engine each user interaction. The system can be tuned by the operator for desired FAR/FRR rate, based on the security requirements of the implementation. Rules can be implemented by the operator based on findings of other customers, or specifically on need/request.

Privacy Protection Mechanisms
BehavioSec does not collect any additional PII data from the user. It analyzes the user's typing cadence, touch screen interactions and mouse/trackpad movements to evaluate whether it is the expected user or fraudulent behavior.
The BehavioSec solution is compliant with all current major privacy rules and regulations, including GDPR.

Investigation and Case Management Capabilities
The typical workflow can be completely automated where the customer's decisioning engine receives real-time data required for high-confidence decision. BehavioSec's solutions are designed to minimize the need for human review and decision-making and data can be fed into any data analysis or visualization tools such as Splunk, Tableau, other case management systems. BehavioSec provides administrative UI for deep behavioral investigations if required.

Management Reporting and User Interface
The BehavioSec provides dashboard as an out of box feature which can be used for reporting purposes. However, the best practice is to integrate BehavioSec data with an existing system or reporting tools.

IMPLEMENTATION

Delivery Model
BehavioSec's delivery model to the market is via both direct sales and channel partners. Will publicly launch a self-serve SaaS offering before EOY'21 (i.e. product- led growth). The offering is currently in controlled release with select partners and customers

Partners
Capgemini, Cisco, Deloitte, Deutsche Telekom, ForgeRock, HID Global, Kount, NEVIS, NICE Actimize, Nuance OneSpan, Ping Identity, Thales

BehavioSec offers cloud-based services in all three models: Managed Services, Private cloud, and hosted services (SaaS) on all major cloud service providers. Professional services team consists of employees with various skillsets and include Fraud Analysts, Data Scientists, Architects, Developers, etc. In addition to the professional services team, BehavioSec has partnered with several System Integrators & Delivery partners to help our customers with the required professional services and support for successful implementations of the BehavioSec platform.

Pricing
Standard Pricing is based on a Per User / Per Year basis and depends on the use case coverage (CIAM/Customer or IAM/Workforce), hosting arrangement, support requirements and other factors.

Transactional based pricing is also available for applicable use cases (e.g., payments)

IAuth Intellectual Property
BehavioSec currently holds about 25 patents. Our R&D team of about 20 employees is continuously working on new innovations to detect and prevent fraud.

Vision & Plan
As the pioneer in providing digital identity and anti-fraud solutions based on behavioral biometrics, BehavioSec envisions a future that is both Secure and Frictionless. To that end, BehavioSec's mission is to continue to refine and develop solutions that solve customer challenges and use cases that include cybersecurity, digital transformation, fraud, and all the associated risks that come with the aforementioned.

Key Differentiators

- Frictionless and seamless security: BehavioSec is 100% invisible to the end-user and provides a frictionless experience and gives no indication to fraudsters how or what's being measured and scored. The solution is designed for high-volume, real- time analysis running entirely in the background.
- Unique User behavioral profiling: BehavioSec platform automatically creates & updates user-specific behavioral profiles right from the first interaction. In each session, user behavior is compared continuously to user specific profile and provide matching score for authentication.
- Advanced fraud detection: BehavioSec can detect effectively wide variety of fraud such as credential stuffing, account takeover attacks, new account fraud, synthetic identities, social engineering, click farms, bot

BioCatch

Headquarters: Tel Aviv, Israel
Founded: 2011
Revenue: N/A
Number of employees: 203

CAPABILITIES

Technology - Behavioral Biometrics

Account Opening
BioCatch protects new account applications by analyzing a user's physical and cognitive digital behavior to distinguish between genuine users and criminals to detect fraud and identity theft and to improve customer experience. This is achieved by profiling user behaviors such as mouse movements, typing cadence, swipe patterns or device orientation and comparing these to patterns observed in population level profiling, to determine statistically observed norms for "good" and "bad" behavior. For example, cybercriminals input data differently from genuine users. They usually don't have the same level of familiarity with the data and are more likely to repeatedly delete and fix errors, rely on copy and paste, or use automated programs for data input. This expertise will present itself with pace and navigation patterns of interaction that are different from those of a genuine user who display the use of long-term memory, hesitate around fields that cybercriminals confidently type in, and will often use the AutoFill feature for some of their personal details.

The BioCatch platform's machine learning algorithms are designed to analyze such patterns and provide customers with a risk score and top risk and genuine factors to be used in the policy manager tool or via API. Using the BioCatch Policy Manager tool, customers can set business and risk policies to determine the appropriate action given the situations (allow, deny, authenticate, review or other custom actions). Activities and sessions that are determined high risk can be sent to review in the BioCatch Cases Manager tool which helps fraud and security operations teams improve and automate incident response. The tool allows customers to improve the efficiency of how they manage fraud cases and alerts marked as high-risk and automate response based on business and risk policies.

Account Takeover
The BioCatch Behavioral Platform leverages machine learning algorithms to analyze physical and cognitive digital behavior of users across digital channels. The model analyzes real-time physical interactions such as keystrokes, mouse movements, swipes and taps, and profiles both genuine users and fraudsters on the user level, comparing them to historical profiles, and on the population level to learn about patterns associated with genuine and fraudulent activity. For example, patterns such as high familiarity with data is associated with genuine users, while high computer proficiency is often associated with fraudulent behavior. In other cases, such as authorized push payment voice scams where fraudsters coerce users to transfer money in real-time while guiding them on the phone, signs of hesitation combined with numerous other fraud indicators suggest high risk activity.

On the user level, BioCatch profiles unique characteristics for each user and compares current sessions to historical profiles to detect changes and anomalies. Fraud and genuine feedback are incorporated to continually enhance the accuracy of the model and adapt to new attack patterns. The BioCatch Behavioral Platform returns a risk score and top risk indicators to provide better visibility into risk. The scores and top risk indicators are used to determine the appropriate action to take. See more information about the policy manager above.

Social Engineering Voice Scams
BioCatch analyses user behavior in real-time to detect when an individual is conducting a transaction under the influence of a cybercriminal, helping banks to protect customers from voice scams and authorized push payment fraud.
BioCatch collects physical and cognitive user behaviors that are turned into powerful insights to identify fraud and identity theft. Analysis is done by profiling users based on physical traits such as typing, mouse movement, swiping and press, comparing current sessions to historical profiles to continuously authenticate users. In addition, BioCatch identifies legitimate usage patterns vs. those of cyber criminals, including human versus automated or bot activity. When session behaviors highly correlate with the known, legitimate user, but some behaviors in the session are abnormal, powerful indicators suggest a person is conducting a transaction under the influence of a fraudster.

BioCatch Inherence for SCA
With over a decade of experience analyzing digital behavior, the BioCatch platform has an unmatched ability to distinguish between genuine users and cybercriminals, protecting organizations and their customers against a broad range of threats. BioCatch takes a fresh approach by monitoring a user's physical and cognitive digital behaviors to detect fraud and identity theft and improve customer experience. Digital behaviors are collected during the SMS OTP flow of the ecommerce journey to create a behavioral biometric profile. BioCatch profiles user behaviors such as mouse movements, typing cadence, swipe patterns or device orientation. The activity is then compared against the historical user profile for the individual account to provide a passive authentication layer and against population level patterns to identify statistically observed norms for "good" and "bad" behavior based on legitimate user and cybercriminal user profiles.

Device Authentication
Profiling characteristics of a device to identify it in future interactions
BioCatch performs device fingerprinting using web and mobile SDKs. Device elements collected for web include IP, IP gelocation, timezone, browser type, user agent string, browser cookie, display settings, permissions, as well as a global unique Identifier use is the BioCatch consortium. Device elements collected for mobile include Mobile ID, SIM, Mobile OS build elements, languages, applications, Bluetooth devices, Wifi, timezone and global unique identifier. Device profiles are incorporated into the various models to detect different types of financial crime.

Fraud Detection
The BioCatch Behavioral Platform leverages machine learning algorithms to analyze physical and cognitive digital behavior of users across digital channels. The model analyzes real-time physical interactions such as keystrokes, mouse movements, swipes and taps, and profiles both genuine users and fraudsters on the user level, comparing them to historical profiles, and on the population level to learn about patterns associated with genuine and fraudulent activity. Applying more than 2,000 behavioral indicators to analyze the online account opening process, BioCatch can distinguish between legitimate, criminal, and non-human users.

Integration Methods
A standard BioCatch integration includes integrating the BioCatch SDKs (Web or mobile) into the client portal/mobile app to collect data for analysis purposes. When users are performing activities (account opening, login, payment, updates, etc.), BioCatch customers send a REST API call upon the need to assess the risk. The BioCatch API will return a risk score, threat indicators, risk and genuine factors and other data points that can be fed into an analytics environment.

Investigation and case management capabilities
The BioCatch Case Manager is designed to be used by fraud operators who are responsible for resolving sessions and activities flagged as high risk. In order to optimize the case resolution process, the BioCatch Case Manager provides supporting information related to session details and risk level. Cases in the Case Manager application are created by automated flagging of risky sessions or activities via the BioCatch Policy Manager. When a policy rule is created, a flag can be set to determine whether a case should be created if a policy rule is satisfied. Once a case is created, it automatically appears in the case queue. The BioCatch Case Manager queue contains all open cases from the last seven days and are prioritized based on date, status, and risk score.

Optimize Fraud Operations
The BioCatch Case Manager offers a methodical comprehensive view of user activity as well as workflow capabilities. Within a case, fraud teams can easily update case status and track resolution progress.
To support case escalation processes, the BioCatch Case Manager complements the BioCatch Analyst Station tool, which is designed to be used by fraud analysts who are responsible for investigating more complex fraud cases or identifying fraud trends. In addition to case resolution actions performed by fraud operators, the Case Manager can be used by Fraud Analysts to investigate escalated cases and surface insights that can be later used to optimize existing policies or create new policies.

Frictionless Experience
Current fraud controls often treat customers like criminals, introducing additional friction into the user experience. This is especially true in the online account opening process where applications are deferred for manual review which can incur high operational costs. Behavioral biometrics delivers better detection of account opening fraud and ATO by understanding behavioral intent to identify illegitimate activity versus that of a legitimate applicant. False declines of applications and transactions are reduced by monitoring user digital behaviors to assess the risk of an activity and driving the appropriate action. The BioCatch solution is designed with customer experience in mind. I t is invisible to the end user, allowing consumers to go about their banking activities while also being guaranteed maximum security.

Continuous Protection
Providing continuous protection is not only about reducing fraud losses but building trust in digital interactions. Unlike other fraud solutions, BioCatch provides truly continuous protection by collecting and analyzing data throughout the session, so even the most subtle changes within the session do not go undetected. The BioCatch Risk Engine is powered by machine learning algorithms that analyze physical and cognitive digital behavior of users across web and mobile channels. The model takes into consideration real-time physical interactions such as keystrokes, mouse movements, swipes, and taps.

Agent User Interface
The BioCatch Analyst Station provides fraud analysts with the visibility they need in order to easily identify, investigate, and act upon potentially fraudulent activity in user accounts. This BioCatch platform component is used to facilitate post-session data analysis whenever an in- depth investigation is required.

Context at a Glance
The Analyst Station automatically reveals critical details related to the latest sessions including risk score, geo- location, threat indicators, user ID, and date and time. By having these key high-level insights readily available, fraud teams can gain context within seconds and kick off deeper investigations with ease.

Capabilities
- Monitor and investigate the latest sessions
- Access detailed session data including BioCatch behavioral insights and threat indicators
- Visualize behavioral anomalies indicative of fraud through video reconstruction
- Leverage advanced query and reporting capabilities
- View risky sessions by geo-location using a detailed map view

Benefits
Optimize fraud investigations with access to detailed session context
Decrease time to action by understanding the exact behavioral indicators that contributed to a session's risk score
Drive complex case resolution using a powerful set of visualization tools
Revel fraud trends via automated query capabilities

Management Reporting and User Interface
Customer reports are custom designed and tailored to their needs. These reports are automatically generated according to the requested cadence (e.g. past week, month, or quarter).

Reporting types include:
- Ad-hoc (i.e. the ability to generate custom aggregate reports on demand).
- Case-level (i.e. records of inquiries, activity, and outcomes for particular applicants or customers).
- User-level (i.e. record of actions taken within the platform by the client's users).
- Session reconstruction is available for all sessions and can be used to analyze behavioral activity. In addition, visualization is available via BI.

IMPLEMENTATION

End User Engagement
- 200M+ Global Users Protected to date with BioCatch
- 60 Global Patents
- 2B+ Sessions Analyzed per Month
- Average 10x ROI reported by customers based on fraud losses

Pricing Models:
Pricing models include 'per API call' and 'per user' based models. Customers can add additional channels for protection (e.g. add mobile to existing web channel) for a % increase on price. Customer can also opt-in to higher level of customer service for a % increase on price.

Key Differentiators

- **Massive Data Advantage** - Leveraging a decade of behavioral data, BioCatch has created the world's largest behavioral insights database, from trillions of behavioral interactions per month from billions of sessions across geographies, entities and use cases across our customer network.
- **Differentiated Value** - Better detection with Behavioral Insights - BioCatch created the category of fraud detection solutions with Behavioral Biometrics, with most banking customers in the space. BioCatch goes beyond behavioral biometrics by delivering behavioral insights through analyzing user behavior on multiple levels:
- **Continuous, Real Time Monitoring and Analysis** - Collection of data and analysis is continuous, providing full visibility into the user activity throughout account lifecycle, from login to logout by providing fraud teams with as score, risk indicators as well visualization tools that provide step by step session reconstruction. Using the Analyst Station, fraud analysts analyze risky sessions and identify patterns to be able to take action quickly to stop fraud before it happens.

Daon

Headquarters: Fairfax, VA
Year business started: 2000
Revenue: N/A
Number of employees: 230

CAPABILITIES

- IdentityX Digital Onboarding: Digital Onboarding offers omni-channel identity proofing allowing for the verification of customers identity documents and biometric information in real time. Enabling customers to establish a trusted identity with their users and allows for the re-use of that trusted identity credential throughout the customers lifecycle.
- IdentityX Authentication: Authentication, the core of the IdentityX platform, provides a wide variety of capabilities across several multi-modal types of biometrics with the flexibility for each client organization to pick and choose those which apply best for their business needs. IdentityX Authentication connects IdentityX Digital Onboarding as well as the FIDO mobile SDKs and Contact Center solutions.
- FIDO mobile SDKs for Android & iOS
- Daon FIDO-standard mobile client SDKs are used by clients globally for mobile app integration to secure the highest-value financial transactions of their end users.

Contact Center-Specific Capabilities
Specialized application of voice biometrics to provide convenience to end users and trust assurance and operational efficiency to the enterprise. Users no longer have to answer knowledge-based questions to prove their identity, less calls need to be forwarded from the IVR system to live agents, but when needed, live agents can save time with caller authentication under 5 seconds and move right to addressing the core needs of their customers.

In-person Identity Assurance: Seamless Travel, and COVID Safety
Binding verified identity credentials with health attributes and other competencies (in particular, COVID vaccine certifications, lab test results, and health questionnaires) as a means of safeguarding and streamlining travel, return-to-work, congregate events, and other in-person experiences. This capability is featured in the world's first widely adopted digital wallet for COVID-19 credentials, "VeriFLY."

These fully integrated components provide identity continuity across the end-user experience. Daon broad expertise allows organizations to offer identity establishment and verification, multi-factor authentication, and recovery across all channels (mobile, web, contact center and physical location). Capabilities of the platform include:

- **Multi-modal**. Supports face, voice, fingerprint, behavioral, and palm biometrics. Vendor agnostic – we can support algorithms of other vendors, ensuring a "best of breed" solution.
- **Liveness**. Supports multiple liveness detection algorithms for face and voice.
- **Policy control**. Includes an Admin Console which supports configurability of all aspects of authentication, such as modality(s), match thresholds, attempts, device capabilities. This provides Daon customers maximum flexibility in balancing convenience for users with the security required for high-value transactions.
- **Multi-tenant**. Allows different population segments (departments, user groups) to be managed independently of each other. With separate administrators and data segregation.
- **Scalability**. Daon core technology has scaled to populations of hundreds of millions. Peak loads of 2,000 authentication transactions per second have been handled with IdentityX.
- **Reliable implementation profile**. Can be deployed in high-availability and disaster recovery configurations.
- **FIDO standard conformance**. IdentityX can be configured as a FIDO UAF and U2F Server and has been certified in this configuration.
- **Flexibility**. Platform independent: Windows or Linux, Oracle, or SQL Server. Runs on commodity hardware - no special requirements. Provides flexible integration options (SOAP/Restful APIs), match-on-server or match-on-device, configurable authentication policies, supports in-band and out-of-band use cases.
- **Cross-channel**. Can be integrated into an enterprise to give a consistent authentication experience across different channels/use cases: mobile, website, ATMs, call-centers, in-person, etc.

Fraud Prevention: IdentityX is designed to work in collaboration with fraud detection tools that gather input from a variety of sources -- including IdentityX -- in order to generate a risk score. Daon platform is designed to maximize interoperability and

has successfully been deployed with a variety of scoring engines, including Ping Identity, ForgeRock, CA Security and Symphonic.

Orchestration: IdentityX offers an array of orchestration and decisioning capabilities, including the ability to: a) intelligently combine multiple authentication factors across different channels and in response to different risk levels, b) intelligently combine algorithms, for instance voice algorithms (both text-independent and text-dependent) or liveness detection algorithms, c) orchestrate rules, factors, and policies within an administration console, and d) set sophisticated onboarding decision rules and workflows. In addition, IdentityX is designed to integrate with 3rd party products to provide additional orchestration, risk decisioning and IAM capabilities. We have established partnerships with several of the leading vendors in the space such as Ping, Forgerock, CA Identity Manager, Nice Actimize and Symphonic. Re-usable connectors are available for many of these vendors and provide detailed authentication results and device signals back to the orchestration platforms for enhanced decisioning.

Knowledge Factors: IdentityX does not provide KBA; IdentityX Onboarding includes an external data check plugin which enables the core platform to call 3rd party APIs and leverage the responses in the decisioning flow.; IdentityX supports both mobile and server-based password/PIN authentication.

Behavioral Biometrics: Daon IdentityX platform incorporates a keystroke dynamics algorithm that analyzes the unique patterns and rhythm of each person's typing habits. While an attacker may know the content to be typed, they will not be able to reproduce the correct keystroke rhythm.

Channel Factors: IdentityX mobile SDKs capture device signals and detect rooted/jail broken and debug status during registration and any point thereafter. This information can be used by a 3rd party risk engine to detect anomalies. IdentityX includes presentation attack detection for both voice and face.

Fraud Detection: Face watchlist capability is built into the IdentityX onboarding solution; no consortium watchlists are used at this time. The default operation of IdentityX is 1:1 biometric matching against a claimed identity. 1:many operations can be performed, depending on customer requirements.

Phone-as-a-token. Supports mobile device authentication to ensure possession of "something that you have" as a cross-channel authentication method originating from another channel (e.g., online web). This can be conjoined with a biometric to achieve MFA.

Voice Biometrics
Daon offers both Text Dependent (Active) as well as Text Independent (Passive) voice authentication.
For TD/Active voice authentication, the process of enrollment is as simple as a user repeating a prescribed phrase three times. Once this is completed successfully, the user simply needs to repeat this phrase at the time of authentication.
For TI/Passive voice authentication, the process of enrollment entails capturing about 30 seconds of conversational speech from a caller, which can occur over multiple calls/sessions. Once this collection is complete, any next attempt for authentication requires between 2 to 5 seconds of speech to confirm a match.

In both cases of voice authentication, the privacy of the user is maintained. Voice samples are converted to a biometric template which is subsequently used for end user authentication. No end user voice samples are stored, and the biometric template cannot be reverse engineered.

In addition, fraud detection capabilities such as liveness detection and continuity are key to protecting the process of voice authentication. Liveness detection prevents the use of pre-recorded speech being played back from a recording device. And voice continuity ensures that not only is the caller authenticated initially but that the same person is continuing to provide information and any instructions to conduct transactions throughout the call interaction.

Authentication & IdentityX Platform
Identity Continuity is the ability to track and provide assurance of an end user's identity through all interactions via any channel. While many vendors provide one or a subset of capabilities, Daon fully integrated IdentityX platform combines the experiences of enrolling biometrics, onboarding and authentication (including contact center agent verification) to provide the most seamless experience for end-users. In addition to the convenience for end users, enhanced risk and trust signals are being modeled utilizing end user trends and behavioral characteristics to enhance the security level of these interactions even further.

Given the significant improvements in digitized biometric capabilities, one of the remaining channels of risk has been contact centers (both IVR and live agents). Fraudsters use social engineering when calling into contact centers to launch account takeover attacks, and this has cost organizations $100s of millions in losses. Pairing identity continuity with strong voice biometrics, Daon contact center offering helps combat and eradicate those fraud attacks. In addition to the foundational voice technologies, a universal voice model (which does not require costly sample collection for tuning the model) will be a key focus area for Daon to apply to authentication and contact center implementations globally.

Finally, the widespread success of Daon client organizations in growing their end user base and overall business call upon further scalability of the IdentityX platform. One current customer benchmark of the platform is achieving 2,000 transactions per second, however Daon is constantly architecting and tuning the system to achieve significantly higher performance levels, both for on-premise as well as cloud-hosted implementations. Existing customers include the largest banks in the world with the highest enterprise transaction volumes, and Daon shall serve these customers well into their future growth.

Scalability
Daon proven operational scale is extremely important. Daon has customers that successfully processed 14 million+ transactions in the last year. Knowing that the digital onboarding solution can provide the same exceptional experience at huge volumes affords customers with the assurance the product can scale with their aspirations.

User experience
Daon utilizes its market expertise to constantly develop its digital onboarding experience. Being able to aggregate the data we see across our customer base means Daon can refine the user experience of what is a historically difficult process for customers. Simpler, more intuitive capture methods for documents and biometrics result in higher conversion, less drop off and most importantly high percentages of successfully verified customers.
Results achieved with deployments:

- **Polarify** – Frictionless eKYC for Japan; Polarify has processed almost 14 million e-KYC transactions in the last 15 months for its customers, who include not just banks, but also some of the world's largest telecommunications e-commerce and insurance companies, including Softbank, Rakuten, PayPay, and Japan's largest life insurance company Nippon Life.
- **New Zealand Government** – Enables a customer to simply and securely verify their identity from anywhere via web, app, or post outlet channels. Before turning to Daon, 43% of New Zealand's users were abandoning the verified identity application process.
- **Capitec** – Fully automated account opening process with instant access to banking functionality. Increase of 28% over the past 12 months to 8.6 million digital banking clients.
- **Esme Learning** – Fast, no-code process for adding biometric identity assurance to online courses (using LTI protocol). Course operators saved an average of 10 Hours per course, thanks to a big reduction in daily admin work.
- **MyPensionID** – Simple mobile app helps pension schemes keep member data accurate and up to date. Pension payments to the deceased is a £1 Billion problem in the UK, which Daon platform helps solve.

IMPLEMENTATION

Delivery Model: Daon go to market model includes both direct and indirect models. Primary partners include sales/distribution as well as technology partners. Depending on region and deal, we will make a decision to either go direct or work with an existing partner.

Partners: Experian, Airata, NICE Actimize, Talkdesk, GEMADEC, ForgeRock, DXC Technology, Deloitte, Avtex, Mitek, DTIS

From an implementation perspective, Daon offerings are geared to serve operational models preferred by our client base. While many clients have on-premise implementations, more commonly the choice is made for a Daon cloud-hosted model. With Daon expertise and economies of scale, our cloud hosted model ensures high-availability and scalability for the growth of client organizations. Globally, Daon Professional Services and Product Support teams include approximately 50 technology professionals distributed globally who provide deep product and industry expertise. Multiple communication channels are used by these teams to disseminate information about the products and to receive input and feedback about experiences in the field.

Pricing:
Daon pricing model includes an annual subscription and can vary by the volume of users. Daon Biometric Research team consists of industry PhD professionals with decades of biometric innovation across the industry. This research team provides innovative methods of authentication and scans the industry for comparative solutions to ensure Daon provides the most accurate and performant biometric offerings. Intellectual property: 160+ patents.

Key Differentiators

- **New customer acquisition and identity proofing**
  With Daon, identity proofing is possible across any channel a business may acquire its customers through. From our native SDKs which fit seamless into any existing application, to our web SDKs and web app which allow a customer to start a journey on desktop, move to mobile for verification, and then hand back to the desktop, we remove all of the friction for the end user. To the customer all it takes is capturing an image of their identity document and capturing an image of their face, but in the background the Daon rules engine is ensuring authenticity in real time and providing all of the users details to our customers backend systems.

- **Account recovery and lost device risk reduction**
  Recovering access to a customer account presents a number of challenges to the business, it has the potential to create a lot of friction and prevent the customer from utilizing the product, but it is also extremely susceptible to fraud. Businesses need to focus on making the process simple for genuine users, but secure against those users who may be attempting fraud. Daon identity platform enables the business to simply capture biometric information from the customer in the form of a selfie, and then compares this to the biometric information captured during onboarding, meaning we can ensure the individual is the same person who opened the account. Re-establishing identity in this manner not only reduces friction on the end user, but reduces the administration overhead on the business, who typically require significant manual intervention to prevent against fraud.

- **Trust elevation of existing users**
  Increasing trust with existing customers can be a very manual process, but utilizing Daon digital onboarding solution, a business can easily user identity verification to migrate a customer from one credential to another. For example, existing customers who use password or MFA to verify their access are easily exposed to fraud and account takeover attempts. Completing the identity verification process means the customer can move from passwords and MFA to using their biometric information to verify access, again providing a simple way to reduce friction while increasing security.

ID R&D

Headquarters: New York, NY
Year business started: 2016
Investment/Funding: ID R&D is now 100% owned by Mitek Systems, Inc.
Revenue: Mitek revenue is publicly available
Number of employees: 50 ID R&D employees

CAPABILITIES

Technology - Voice Biometrics

Core Authentication
ID R&D's core voice biometrics product, IDVoice®, is a robust speaker recognition engine with the industry's highest accuracy. ID R&D is a Core Technology provider for the industry. The original proof point of accuracy is the NIST 2019 Speaker Recognition Evaluation in which ID R&D placed 1st out of 52 participants. Others in the competition included Nuance and Pindrop. The most recent proof point is ID R&D placing 1st out of 21 participants in the Interspeech Short Duration (1 to 5 seconds) Speaker Verification Challenge 2021 in March. This challenge included speakers enrolling in one language and verifying in another language.

ID R&D uses the same core engine for both Text Independent and Text Dependent. The only difference is the enrollment. TD requires the user to say a short passphrase 3 times. TI enrollment is with longer utterances. There is no need to change engines. Other features include:

- Language independence
- Accent independence
- Model enrichment to adapt to changes in the voice over time
- Cross-channel compatibility, enabling enrollment on a 16 kHz microphone channel and verification on 8 kHz telephone channel and vice versa.
- Out-of-the-box performance with no data collection, no background models to create, no training based on the spoken content

The IDVoice SDK also includes gender and age analysis. A key derivative feature is Diarization, the ability to separate speakers in a call recording. This is a valuable feature when working with call center data that is often recorded monophonically. With diarization, a company may harvest their previous call recordings to extract audio for enrollment.
ID R&D Diarization accuracy was a key advantage in a large call center account that first chose a vendor based on size and reputation. The other vendor was unable to achieve the expected enrollments three months after winning the contract. The deal was then granted to ID R&D's partner. That project went live with ID R&D in January 2020.

The strength of the cross-channel performance allows the company to support both call center and mobile use-cases including integrations with chatbots and messaging platforms.

Text Dependent
For Text Dependent enrollment, users speak a passphrase. Enrollment requires a phrase of at least 0.6 seconds for the microphone channel, although more is recommended, and 2 seconds for the telephone channel.
Recent performance breakthroughs achieved by the ID R&D team allowed the IDVoice product to meet the necessary security guidelines to be used by device manufacturers as a core device unlock security factor. For the first time in mobile device manufacturing, voice biometrics may be deployed on device not only as a convenience, but as a security measure. ID R&D has numerous customers for the device unlock use case. Text Independent uses the same internal engine.

Minimum Authentication Net Speech Requirement: 1.5 seconds
Minimum Enrollment Net Speech Requirement: 15 seconds

ID R&D offers a stand-alone application for Fraud Detection targeting Telco clients. The objective of this software is to batch-mode process call center recordings of the Telco's new subscribers. The software compares all new subscribers to voices of known fraudsters, and it compares all new subscribers to other recent new subscribers to ensure that each new subscriber has a unique account. If a new subscriber has the same voice as two other subscribers, all these records are flagged as potential

fraud. This is a highly targeted fraud solution now being sold by Thales Group to their telco audience. Thales serves 75% of the telcos worldwide.

Synthetic Speech Detection Capabilities
ID R&D brings leading liveness capabilities to the market for both Presentation Attacks and Synthesized Speech Detection. ID R&D provides Voice Anti-Spoofing. It scored first place in the most recent ASVSpoof.org anti-spoofing competition in 2019. This technology works with 16 kHz audio. Furthermore, for embedded solutions, ID R&D combines anti-spoofing into the voice matching as a sub-network. The result is high accuracy in a more compact size and lower latency than deploying each product separately.

Results of recent benchmarks
NIST SRE 2019: ID R&D achieved the best result among 52 participants.
ASVSpoof 2019: ID R&D achieved the best results among 49 participants.
SdSV Challenge 2021: ID R&D achieved the best result among 21 participants.

Approach to tuning, calibration, and optimization of end-user implementations
Tuning at the end-user is typically required for older generation technologies. ID R&D's neural network technology relies on training in advance of deployment. Calibration may sometimes be useful but is generally not necessary.

IMPLEMENTATION

End User Engagement
Delivery is through a channel partner. As a technology component provider, ID R&D does not offer products for end-customer consumption. Cloud-based services are offered directly only for testing and evaluation. Several of our channel partners deploy our software and offer it as a cloud-based solution.

Pricing: Per transaction ($0.005) OR per user/per month with unlimited transactions.

Vision & Plan
For Enterprises, consumer adoption will help them pass a tipping point. But there may be another reason that Enterprise adoption increases on mobiles. The reason is security.

Enterprises testing security options today would like to use fingerprint or vein or iris, all proven to have low false acceptance rates of impostors. But none of these technologies, according to our partners, are reliable when implemented using a mobile device camera unless the mobile has special hardware. Adding hardware is fine for narrow use cases but not practical for large-scale adoption. So that means if the Enterprise wants more security factors, they will have to use what will work with the preponderance of mobile devices. The additional factors must work with the standard types of cameras and microphones available on mobile devices, including lower-end devices. The two only viable biometric factors with these constraints are face matching technology and voice biometrics.

ID R&D's focus, therefore, is on delivering security-level voice biometric accuracy so voice may become an Enterprise-grade factor for security.

ID R&D's voice biometric technology is in the process of getting teed up for large-scale consumer deployments on mobile / consumer electronic / IoT devices. Therefore, we expect the next breakthrough in voice biometric adoption to come not through a call center, but through adoption by device manufacturers and other hardware producers. ID R&D has developed new biometric products (with smaller footprint and latency) to meet the technical requirements of such customers. In the Enterprise world ID R&D already has some companies proceeding directly to Enterprise-grade biometric deployments of voice for security (Wicket.com). Mitek Systems also will be leading the way forward to show the value of voice for Enterprise security. The total available market for voice on the mobile to greatly outweigh the value of voice authentication in the call center.

ID R&D believes what will happen in the five to ten-year timeframe is that voice on the mobile will be the IT priority over voice in the call center. Then the call center will eventually need to work with voice on the mobile, and that will mean call centers will likely migrate to whatever is in the mobile app instead of the other way around. Or it's possible they will never meet, simply because the cost and complexity of call center integration prevents wider adoption of voice biometrics.

Key Differentiators:
- Voice biometric accuracy as demonstrated by NIST and SdSV challenge
- Voice anti-spoofing accuracy in the microphone channel as demonstrated by ASVSpoof
- Latency and size for mobile and embedded applications (150 ms, 10MB) to achieve the highest accuracy

LumenVox LLC

Headquarters: San Diego, CA
Year business started: 2001
Year IAuth market contribution started: 2017
Investment/Funding: $12M
Revenue: N/A
Number of employees (directly related to IAuth): 57 employees

CAPABILITIES

Technology - Voice Biometrics

Core Authentication
Text Dependent
LumenVox offers text dependent technology as part of our Multifactor Authentication Platform (MAP) which caters for any language and phrase. We have several languages and phrases available out-of-the-box e.g. “my voice is my password”. The technology can be integrated with our Workflow Manager solution which provides clients with the ability to create custom IVR call flows to support text dependent enrolments and verifications. The technology also incorporates a hybrid model that is used for text dependent enrolments into the text independent engine, facilitating quicker text dependent deployments. The technology is deployed utilizing Kubernetes technology so allows for easy deployment and scaling.

Text Independent
LumenVox offers text independent technology and supports any language. The technology is also built into our MAP platform and can be implemented with our Agent Desktop interface, which allows for easier client integration. The technology also fits seamlessly into our Fraud Scanner solution for online matching of live calls against a fraudster watchlist. The technology is deployed utilizing Kubernetes technology so allows for easy deployment and scaling.

- Minimum Authentication Net Speech Requirement: 3-5 seconds
- Minimum Enrollment Net Speech Requirement: 20-60 seconds

Fraud Detection
- Watchlist: Up to 1000, recommended is around 500
- Cross matching: Capability as part of fraud offering
- Typical workflow: Fraud can be detected using our batch Fraud Scanner product where audio is loaded as a batch file and compared to a fraudster watchlist. Fraudsters can also be detected online whilst a speaker has been verified using our text independent Call Centre Suite product.
- Presentation Attack Detection Capabilities: Software has playback detection features providing alerts if the audio is similar to other samples previously presented to the engine.
- Synthetic Speech Detection Capabilities: Feature of the text independent technology

Approach to tuning, calibration, and optimization of end-user implementations
Tools are available for clients to perform their own calibration and tuning.

Management Reporting and User Interface
- A management console is available for active, passive and fraud solutions. The following console as part of the Multifactor Authentication Platform (MAP) allows super users to:
- Change configs
- Maintain voiceprints
- Listen to audio recordings for troubleshooting
- Obtain reporting
- View error logs
- Management consoled dashboard
- View enrolment and verification transactions
- View transaction details and listen/download audio
- Update configurations

Fraud Scanner
This portal allows users to:

- Change configs
- Upload audio into a fraudster watchlist
- Upload audio batches
- Create/schedule a job to run a batch against a watchlist/s
- View results

Solution
LumenVox offers a fully integrated multi-modal, multi-factor (including voice biometrics) password reset solution. The solution integrates into most authentication platforms. Also offer a windows pre-login solution that allows users to utilize multiple modalities including voice biometrics to login to various applications. Workflow Management software allows clients to implement active voice biometric solutions with ease, allowing them to create customized IVR call flows. Call Centre Suite solution incorporates various text-independent technology components such as our Multifactor Authentication Platform, agent desktop application, call recorder into one easy-to-implement solution.

IMPLEMENTATION

Delivery Model: Direct and through channel partners
Primary partners: Avaya, Genesys, CISCO, Enghouse Networks, SpinSci, Capgemini, Kyndryl, CSG, Twilio, Five9, Ring Central, Allianz, Interactive Northwest, Telnyx, Fiserv, Alvaria

Product works in a cloud environment (public, private or hybrid cloud model). Also work with an array of partners including professional service partners who deliver solutions to our end customer.

Pricing: Flexible pricing based on subscription or usage/transaction models. They are all term licenses.
Over 30% of the company is focused on R&D. LumenVox holds 18 patents in the area of voice biometrics

Vision & Plan
To develop and streamline the deployment of the world's most comprehensive voice enabled technology. The broad portfolio of AI-driven speech products is designed to power voice interaction for a diverse ecosystem of network partners and application developers, and made available for on-premises, multi-cloud and hybrid environments.

Key Differentiators

- **Flexible** – The software allows for easy integration compared to other competitor products. Our technology along with various ancillary components allow for easy integration without the end client having to undertake a large amount of development. The software supports a wide range of client use cases.
- **Scalable** – The software can easily scale to any size deployment. The software make use of microservice technology.
- **Accurate** – on par or better than competitors as determined through our partner analysis

NICE

Headquarters: Raanana, Israel
Year business started: 1986
Year IAuth market contribution started: 2016
Revenue: $1.7B
Number of employees (directly related to IAuth): 80

CAPABILITIES

Technology - Voice Biometrics

Text Dependent: NICE authentication solution supports the option of active enrollment and active authentication.
Text Independent : The NICE authentication solution is completely passive; the call is streamed to the voice biometrics engine for authentication. The TI VP can be used during a live call or on self-service channels like IVR/mobile (NICE Single VP technology).

Minimum Authentication Net Speech Requirement: 3 sec
Minimum Enrollment Net Speech Requirement: 30 sec

Fraud Detection: Enables the creation of multiple watchlists of up to 5000 voiceprints. These are scanned during the enrollment process to prevent enrolment of known fraudsters and to block known fraudsters during a live call.

Cross-Matching: Uses AI, voice biometrics, and advanced analytics to continuously and proactively detect fraudulent behavior and expose unknown fraudsters across millions of calls over time. Calls are scanned to identify fraudulent behavior and match the voiceprints of fraudsters calling multiple times to single or multiple accounts. A prioritized list of probable fraudsters is provided to the fraud team for investigation. Verified fraudsters are added to a watchlist and future calls to the contact center are blocked.

Describe a typical workflow: Provide multiple layers of call analysis – from analysis of a single call to analysis of millions of calls - thereby providing a comprehensive solution to effectively fight fraud:

- Single call analysis
- Every live call is compared in real time to the watchlist of known fraudsters.
- In the event of a match, an alert is provided to the agent, who then applies the formal procedure for such cases.

Synthetic Speech Detection Capabilities: Based on deep neural networks, NICE's proprietary synthetic speech detection engine uses advanced deep learning technology. For the enrollment process also, just before a voiceprint is created, the caller's voice is compared to the watchlist of known fraudsters to ensure a known fraudster is not enrolled.

Millions of calls analysis – Behavioral analytics automatically detects high-risk interactions based on a unique fraud model, scanning millions of calls coming into the contact center. Voice analysis exposes unknown fraudsters by clustering voiceprints of the same person and creating a prioritized list for the fraud team to investigate. The fraud team investigates highly suspect fraudsters and, upon confirmation, adds their voiceprints to the watchlist so that they can be blocked them in real time if they call again. This fully-automated solution eliminates the time-consuming manual work of fraud analysis teams by enabling them to focus on exposed fraudsters – while keeping consumer data safe significantly, cutting fraud losses, and preserving brand reputation.

Presentation Attack Detection Capabilities: NICE has a proprietary playback detection engine that uses advanced deep learning technology and is based on deep neural networks.

Results of recent benchmarks: NICE has benchmarked its solution with ASVSpoof, DeepHorizons, Blizzard, and Wavenet. We achieved 75-80% accuracy with a False Positive of 0.1%.

Approach to tuning, calibration, and optimization: The NICE voice biometric engine and spoofing engines (synthetic and playback) can be calibrated and tuned to archive business FAR/FRR needs. This takes place on a set of calls prior to go-live, to identify the optimal working point (threshold) of the engines. After go-live, the KPIs are monitored, and additional fine tuning is applied as needed to achieve maximum business value.

Agent User Interface: Provides an API that enables integration with CRM applications. For faster OOB deployment, NICE provides a desktop web app client (IntelliAgent) that seamlessly integrates with the solution.

Management Reporting and User Interface: NICE provides a platform with application suites that enable our customers to configure the solution, search and listen to calls, and manage fraud watchlists and voiceprints, and an investigation tool in which the prioritized list of exposed fraudsters appears with all their related information.
Technology - Behavioral Biometrics

User Authentication
NICE's vast portfolio includes market-leading solutions for caller behavior and speech analytics, infusing our fraud prevention solution with insights on user behavior. Using deep neural networks and machine learning, these behavioral and contextual insights are leveraged to improve the authentication and fraud prevention process, enabling agents to focus on providing excellent service for legitimate clients, while stopping fraudsters before they cause harm.

Device Authentication
The NICE authentication solution offers further out-of-the-box device authentication capabilities, that include:
Number spoofing detection - Detecting whether the calling number is spoofed and alerting the agent accordingly
Virtual device – Identifying calls being made via a virtual device and not a physical device (that has a “real” number)
Number recently ported – Detecting phone numbers that have recently been ported (e.g. in the last few hours), which could indicate fraudulent behavior

Fraud Detection
NICE Enlighten AI technology is used in the fraud solution to interpret and measure the human behaviors and actions that represent fraudulent activity. It leverages voice biometrics to make comparisons across millions of voice interactions to reveal probable fraudsters. Engine was able to detect 85% of the suspicious behaviors in a call flow.

Approach to scoring, tuning and calibration: AI model has been fine-tuned and calibrated based on millions of calls in major enterprises. During the implementation phase, we are adding additional behaviors based on customer inputs and the AI engine. Model doesn’t use any PII information for model creation.

Investigation and case management capabilities
As part of fraud prevention solution, NICE provides an investigation tool to investigate the relevant interactions of probable fraudsters. Specialists and investigators can view the dashboard with high-risk fraud behavior indicators, metadata, recordings, and relative scores. They can review the information and play back the calls, and upon confirmation, can add the newly exposed fraudster’s voice to the watchlist. They can also customize scores per line of business and adjust thresholds to accommodate the organization’s unique fraud environment.

Management Reporting and User Interface investigation tool combines various risk factors, including behavioral and voice biometrics and more, in order to provide relevant reports and investigation tool.

Platform
The NICE authentication and fraud prevention solution is based on NICE core technologies and assets. Recorded interactions serve as the substrate foundation for automatically and systematically creating clients’ voiceprints. The authentication solution is used to automate the authentication processes and guide agents in real time. These core technologies are intertwined together with voice biometrics to comprise a robust yet seamless and passive real-time authentication. NICE leverages its deep experience and understanding of the contact center ecosystem and is the only authentication solution that covers unique and complex contact center call types, such as multi-beneficiary or on-behalf calls.

Enrollment:
The NICE solution has two primary options for enrollment: Option one is passive enrollment with a live agent, leveraging natural conversation to seamlessly collect audio for enrollment. Option two is historical enrollment, using NICE's patented solution. The ability to use historical calls for enrollment purposes enables NICE Real Time Authentication (RTA) to perform mass-enrollment of callers, in advance. NICE RTA is then ready to authenticate these callers on day one. In addition, NICE RTA supports the option of Active enrollment.

Authentication:
NICE RTA is completely passive; the call is streamed to the voice biometrics engine for authentication. Single voiceprint technology allows for consistent authentication and enrollment across all customer service channels, including mobile, IVR, virtual agents, voice, etc. NICE RTA employs additional validation capabilities and supports complex call center scenarios such as:

- Speaker Change Detection – enables re-authentication at any time during the call if the speaker has changed.
- Deep Fake Detection – deep neural networks detect and expose fraudsters using deep fake technologies to mimic user voice.
- Replay Attack Detection – AI capabilities detect fraudsters playing a recorded voice.

- Multi-factor Authentication (see below)
- Multiple Beneficiaries – For accounts with multiple beneficiaries, the solution determines if the caller is indeed one of the beneficiaries and authenticates them.
- Authentication On Demand – provides the ability to use the authentication request *again* during a call, for scenarios like an on-behalf call, a speaker change during a call, step-up authentication, etc.

Multi-Factor Authentication and Orchestration (Decision Making):
In addition to voice biometrics and behavioral analytics, NICE RTA offers further out-of-the-box multi-factor capabilities, including:

- Number spoofing detection – Detecting whether the calling number is spoofed and alerting the agent accordingly
- Virtual device – Identifying calls being made via a virtual device and not a physical device (that has a "real" number)
- Number recently ported – Detecting phone numbers that have recently been ported (e.g. in the last few hours), which could indicate fraudulent behavior.

These factors are prioritized and optimized using a proprietary decision-making engine that determines the optimal method for authentication for each interaction scenario between callers and agents. Factor optimization enables leveraging multiple factors in a cost-effective and robust manner, to effectively authenticate and reduce fraud, while providing the best customer experience, optimizing costs, and maintaining compliance with multi-factor authentication regulations.

Fraud Prevention:
The Fraud Prevention solution enables detection and blocking of known fraudsters, as well as exposure of previously unknown fraudsters. Each additional fraudster's voiceprint is added to the fraud watchlist that is used in real time to compare a caller's voice to all the voices in the watchlist. In case of a match, the agent receives a real-time notification, and the fraudster is blocked.

NICE's market-leading Proactive Fraudster Exposure (PFE) solution is now further augmented with AI and analytics, as part of Enlighten AI for Fraud Prevention. This innovative, AI-powered, self-learning solution continuously detects fraudulent behavior across millions of calls. Identifying calls with patterns of risky behavior, it zooms in on those calls with PFE's voice biometrics technology, to expose fraudsters attempting to authenticate into or take over consumer accounts. Probable fraudsters that are exposed are sent to the fraud analyst team for further investigation and, upon confirmation, their voiceprints are added to the fraud watchlist, which will block them from contacting the contact center in the future. This fully-automated solution eliminates the time-consuming manual work of fraud analyst teams, by enabling them to focus on exposed fraudsters – all while keeping consumer data safe, cutting fraud losses significantly, and preserving brand reputation.

The solution offers a friendly investigation tool in which the prioritized list of exposed fraudsters appears with all their related information, such as caller ID, call time, risk score, the factors that drive the score, etc. The investigation tool enables the fraud team to quickly find all the information they need, as well as listen to each suspected fraudster's interactions at the click of a button.

When the voice of a fraudster on the fraud watchlist is identified, a real-time notification is generated on the agent desktop either through a dedicated API which connects to the CRM platform, or through NICE's agent desktop app, IntelliAgent.

Behavioral Factors:
NICE's vast portfolio includes market-leading solutions for caller behavior and speech analytics, infusing RTA with insights on user behavior. Using deep neural networks and machine learning, these behavioral and contextual insights are leveraged to improve the authentication and fraud prevention process – enabling agents to focus on providing excellent service for legitimate clients, while stopping fraudsters before they cause harm.

Integration Options:
NICE authentication and fraud solutions provide a variety of integration options, including an API into the platform (Connect API) which enables easy integration of CRM/ IVR/ mobile apps with the solution. For those seeking a quicker solution, there is a desktop web app client (IntelliAgent) that seamlessly integrates with the solution and dramatically reduces deployment time. NICE authentication and fraud solutions integrate with Actimize Risk Case Management, sending fraud alerts in real time for analysis by the fraud/ security team. NICE authentication and fraud solutions also integrate with Nexidia Enlighten AI models and can leverage additional behavioral factors as part of their fraud prevention capabilities. The solution now enables flagging of high-risk calls for analysis using a simple rule-based mechanism for call collection.

Applications and Reporting:
NICE provides a management application that enables configuring of the solution according to customer needs. The solution provides the ability to manage the fraud watchlist and fraudsters' voiceprints.

NICE Busines Analyzer:
Enables searching for and listening to calls, based on user queries.

Authentication Spotlight:
NICE offers a dashboard that displays trends and solution efficiency. Its main areas are customer enrollment, customer consent, and authenticated calls, which are further broken down into time frames. Since the authentication solution works behind the scenes enrolling customers and authenticating calls, its value to the organization is not immediately apparent to business users. The Authentication Spotlight gives these business users a clearer picture – how many customers have been enrolled, how many have been authenticated, and where there are issues in the process.

NICE PFE (Proactive Fraudster Exposure):
PFE is a user-friendly investigation tool in which the prioritized list of exposed probable fraudsters appears, with all their related information. The list is created by leveraging voice biometrics and AI technology to cluster voiceprints that repeatedly call the contact center.

NICE Reporter:
This application provides built-in report templates that enable users to customize their report and have them delivered on a scheduled basis.
For advanced users, the **NICE DB Kit** provides a set of DB views that enable access to NICE data warehouse, for advanced reporting based on DB data.

IMPLEMENTATION

Delivery Model: Both channel and direct
Primary partners: Global
Service management: Cloud and hosted as part of the NICE CXone offering
Size of professional services team: Based on requirements, as multiple teams support multiple products
Pricing: Perpetual license, Subscription (Term), or SaaS - depending on the deployment model
IAuth intellectual property: https://www.nice.com/patents/

Vision & Plan
NICE will continue to lead the market with voice biometrics technology and powerful AI capabilities that help customers proactively fight against fraud. NICE plans to further extend these capabilities to remain several steps ahead of fraudsters, while delivering the best customer experience for contact center callers and agents, through every channel.

As the world leader for contact center services, NICE is working to expand its integrated voice biometrics solution as part of the NICE CXone CCaaS offering with additional capabilities and integration with other NICE products and technologies that will enable NICE to provide the following:

- Integrate biometrics with other NICE services, like AI and analytics, for an improved authentication process
- Use “big data” from all customers to create a consortium of voices of imposters and suspicious behaviors for the benefit of all customers
- Connect to NICE Actimize, a world leading financial fraud solution in the digital channels and create a synergy between the solutions for the benefit of customers in all voice and digital channels

Key Differentiators:

- **Native CCaaS voice biometrics solution** as part of the leading CXOne CCaaS offering, enabling ultra-fast ROI with 3-4 weeks' time to value.
- **Scanning millions of calls to expose unknown fraudsters** - The NICE fraud prevention solution automatically and continuously scans millions of calls, detecting and exposing unknown fraudsters daily.
- **Historical enrollment (NICE Patent)** - Using one-of-a-kind historical enrollment, the solution can enroll most customers before go-live, for quicker ROI.

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.

Neustar

Headquarters: Reston, Virginia
Year business started: 1998
Investment/Funding: Golden Gate Capital (recently announced TransUnion acquisition)
Revenue: N/A
Number of employees: 200

CAPABILITIES

Technology - Network Authentication and Fraud Detection

Carrier Partnerships: United States and 10 countries.
Device or number-based Partnerships: United States and 33 countries

Number/Device Reputation
Neustar has a rich repository of phone attributes and identity to phone attributes. Neustar can expose a subset of these attributes to Neustar customers. For attributes that cannot be exposed Neustar leverages these attributes in Phone Reputation scores that created using machine learning models and the scores are exposed to customers.

Number/Device Ownership
Carrier Partnerships for SIM/SWAP mitigation Neustar has direct connections to carriers and partners to get carrier data including SIM swap. Neustar has its own phone ownership data for Canada and United States.

Detection Capabilities
Neustar possesses data that indicates the time when phones are being used therefore indicating unusual activity.

Approach to scoring, tuning and calibration
Neustar utilizes expert knowledge and customer provided disposition data to identify fraud to train machine learning models. Because of Neustar's large repository of telephony and device data Neustar is able to build many machine learning models with different permutations of data/variables to detect the same fraud and determine which models and variables perform the best. These models are converted into runtime code to be used in production which enable Neustar to return predictions within 100ms. Models are monitored for degradation and rebuilt when we see their degradation goes below a certain threshold.

Management Reporting and User Interface
Neustar uses Kibana for customer facing reporting and dashboarding.

Authentication Solutions
For callers originating their calls from unique physical devices, such as mobile phones and residential cable and landlines, Neustar Inbound Authentication confirms that the calling phone is engaged in a call with the call center through a real-time deterministic inspection of the call and calling device. Successful inspection results in delivery of an ownership/device authentication token. Callers using common vectors of call center fraud are never authenticated. Callers that pass inspection experience significantly fewer KBA questions and can be trusted with higher-value options within an IVR.

For the balance of calls that don't originate from unique physical devices, Neustar Inbound Authentication leverages results from its history of inspecting billions of calls and additional data about phone numbers, carriers, and network routing from its role as a licensed telephone carrier. The results allow for the stratification of caller treatment by trust level.

A small percentage of these calls (one to three percent) may be sent for closer scrutiny, along with many of the signals that drove their probabilistic risk assessment scores. Call outcome results, shared via a client feedback community, continuously improve detection rates and reduce false-positive rates over time.

Customers often call from a number other than the one in their CRM record. Neustar Inbound Authentication instantly identifies unknown callers using the Neustar OneID system, allowing you to match the consumer to your CRM and reduce time-consuming caller identification efforts by agents or in the IVR. When appropriate, containing more calls within the IVR not only improves the efficiency of your operations, but also frees live agents to interact with high-value or high-need consumers. Neustar Inbound Authentication reduces fraud risk, improves customer experience, speeds call resolution, and reduces IVR-to-agent transfers.

IMPLEMENTATION

- Delivery Model: Both direct and channel
- Primary partners: Call Center: NICE, Nuance, Avtex, Coop, Altigen
- Offer via a private cloud
- Pricing: Vary by transaction volume
- IAuth intellectual property: Patent #'s – 8,238,532 | 9,001,985 | 9,264,536 | 9,762,728 | 9,871,913

Vision & Plan
In 2022 plan to add support for STIR/SHAKEN as a way to isolate spoofed from non-spoofed calls. As criminals continue to migrate from spoofing to virtualized attacks (attacks from non-physical sources such as Google Voice, Pinger, VoIP resellers, etc.) adding new signals to both detect these calls and to separate those from trusted callers from criminals.

Key Differentiators:

- Only ownership-factor authentication service for the call center. Uses patented network forensic inspection to determine with 100% confidence that phone calls are legitimate and not spoofed, hacked, manipulated, or virtualized.
- Only solution to offer automated caller identification for unknown ANIs using OneID repository. No other service can identify a caller and validate the call.
- Only pre-answer signal available to identify high-risk calls. Other solutions require engagement with the caller or can only deliver post-answer solutions

Phonexia

Headquarters: Brno, Czech Republic, European Union
Year business started: 2006
Year IAuth market contribution started: 2017
Investment/Funding: Self-funded
Revenue (either estimated or publicly available): USD 3.1M
Number of employees (directly related to IAuth): 65

CAPABILITIES

Technology - Voice Biometrics

Core Authentication
Text Dependent: Phonexia technology supports text-independent scenario by default.

Text Independent: Passive verification provides better CX and stronger security at the same time. Phonexia Voice Verify is language independent, so different languages and phrases can be used during enrollment and verification, and the technology will still deliver the greatest results.

Minimum Authentication Net Speech Requirement: 3 seconds
Minimum Enrollment Net Speech Requirement: 20 seconds

Fraud Detection
Currently present in a GOV product called “Orbis” for Police/LEA. For commercial use, broader fraud use cases handling is coming in 2022.

Watchlist: 1:n comparison – no cap, depends on underlying HW

Cross matching: n:m comparison – not in production, coming in 2022

Describe a typical workflow

- LEA/Police have legally obtained voice samples (recordings) of persons of interest.
- LEA/Police feed the voice samples into Orbis & add attributes and categories.
- Legally obtained surveillance audio is fed into Orbis.
- Orbis finds persons of interest’s voices in surveillance audio so that police personnel do not need to listen manually to 1000s of hours of surveillance audio but can only focus on the recordings where persons of interest are identified.

Presentation Attack Detection Capabilities
No specific functionality currently in production – relying on the performance of the biometry system
Specific functionality coming in 2022

Results of recent benchmarks: Second place in the VoxCeleb Speaker Recognition Challenge 2021 (VoxSRC-21) – Track 3 Self-supervised speaker verification

Tuning, Optimization, and Calibration
The system comes with a default calibration profile. Within the initial deployment, we offer the creation of a customer-specific calibration profile free of charge – to match system performance to a customer's audio input specifics & to match the customer’s acceptance criteria. Re-calibration based on a customer request after a specific timeframe is included in the maintenance & support package or can be agreed upon ad-hoc. Within the initial deployment, we also offer an option to find the right FAR/FRR setup.

End-user Implementation
Provide 2 standardized product packages depending on needs and the scaling requirements of the customer.
We provide comprehensive implementation documentation and a range of services – from courses/learning sessions, tutorial documents & videos to guided or Phonexia-performed deployments. For integration, our product offers REST APIs & supports a variety of technologies & protocols to match the customers' needs (SIP/RTP, HTTP(s), WebSockets, Webhooks).
Beyond that, customers can opt into a maintenance & support package.

Agent User Interface: On the Phonexia Voice Verify roadmap for 2022

Management Reporting and User Interface
All products offer standard API access & possibilities for all gathered logging and telemetry data to be fed into data analysis and visualization tools based on the customer's preference. On top of that, Phonexia Voice Verify offers state-of-art tools (incl. interfaces) for advanced users & admins to get information/reports from logs, allowing monitoring of the whole system & services (Kibana, Grafana).

Decision Making Approach: Authentication is determined by reaching a threshold based on a likelihood ratio score.

Integration
Phonexia Voice Verify is typically integrated between PBX & CRM or Contact Center software Both integration connections are supported by the REST API.
The PBX connection can be established using:

- SIP/RTP
- RTP payload over a WebSocket
- Using HTTP(s)

Enrollment & Verification verdicts are available via webhooks for fast & effective communication between connected systems.

IMPLEMENTATION

- **Delivery Model**: All PoCs that Phonexia Voice Verify is currently having are delivered together with Phonexia partners.

- **Primary partners**: Superbo.ai, AudioCodes, Almawave, ITNG, NTT. Phonexia Voice Verify supports on-premises as well as cloud and private cloud deployments (incl. biggest cloud providers like Amazon, MS Azure & others).

- **Pricing**: The default pricing structure is pay-as-you-go pricing on a monthly basis. Pricing is based on the number of interactions (the number of enrollments or verifications made). Based on customer requests, we also support yearly pricing or a flat-rate model based on an individual agreement.

- **IAuth intellectual property**: 20 employees at R&D who work closely with the Speech@FIT research group of the Brno University of Technology.

Vision & Plan
Key product strategy pillars:

- Keep & develop voice biometry leadership through an ongoing commitment to research.
- Continuous work on differentiators below.
- Broaden fraud prevention use cases coverage.
- The synergy between GOV & COM use cases and functionalities facilitating them.
- Invest into scalability and enterprise-level security.
- Voice Biometry as a Service.

Key Differentiators

- **Reliable caller verification in 3 seconds:** Phonexia voice biometrics technology leverages state-of-the-art deep neural networks specifically designed to provide highly accurate verification of extremely short speech.
- **Quick to Evaluate:** Phonexia Voice Verify can be tested via a demo today, your developers can explore its capabilities through a sandbox tomorrow, and a PoC can be finished in just a few weeks.
- **Closed-Loop Support That Cares:** Phonexia support engineers are very close to dev engineers, so that they can provide a quick and accurate resolution.

Pindrop Security Inc.

Headquarters: Atlanta, GA - USA
Year business started: 2011
Investment/Funding: $213M through ($90M Series D / Vitruvian Partners Google Ventures and Andreeson Horowitz)
Revenue: N/A
Number of employees (directly related to IAuth): 235+

CAPABILITIES

Technology - Voice Biometrics

Core Authentication
Text Dependent
Pindrop Passport, a multi-factor authentication solution does not use a text dependent biometric authentication approach. Pindrop's approach is agnostic to speech, keywords, language or spoken text and instead focuses on the voice characteristics itself (amongst other factors). A text dependent approach, in our assessment, limits enrollment, adds friction and is vulnerable to errors.

Text Independent
Pindrop Passport is a multi-factor authentication solution. One of the factors is Voice leveraging Deep Neural Network (DNN) based Pindrop Deep Voice biometric engine provides text, language and speech independent voice enrollment and authentication. Voice Authentication capability in omni-channel environment: Recently Pindrop extracted out the Deep Voice Engine that has had proven success in call channel (IVRs and agent leg) and offered it as a SaaS service that enables customers to voice authenticate users in all channels. This service enables customers to run enrollment campaigns from mobile channels or enroll users with existing call recordings. It also enables customers to enroll consumers on any channel and authenticate them in any other channel as well.

Short Utterance Text Independent Authentication
Minimum Authentication Net Speech Requirement: Pindrop Passport does not require a minimum net speech requirement since (i) voice is not the only factor we use. In the absence of speech Passport can leverage other factors such as behavior, carrier metadata, device, caller ID, risk to authenticate (ii) Passport can authenticate in very low speech environments such as IVR, with net speech availability of <1 second.

Minimum Enrollment Net Speech Requirement: Passport does not specify a minimum enrollment speech requirement. As mentioned above, Passport can authenticate callers without previously enrolled voiceprints by leveraging multiple factors. Even within the context of voice-based authentication, Passport powered by Deep Voice, can authenticate callers with <1 second speech availability.

Fraud Detection
Watchlist
Pindrop Protect fraud detection solution leverages both the customer provided fraudster watchlists / blacklists as well as proprietary fraudster data and Pindrop Consortium to perform one-to-several comparison of incoming call risk.

Cross matching
Pindrop Protect leverages Trace graph algorithms to perform a risk assessment of multiple data points (call, ANI, accounts). This risk assessment can be used to match call risk with account risk on a 1:1 or 1:n or n:n levels.

Describe a typical workflow
Protect delivers feedback on each call as it learns more about the call. Risk is assessed passively and continuously while a call is in-progress. As calls come through a call center's infrastructure, they are analyzed by the Protect solution for their individual Phoneprinting® classifiers. These Phoneprinting classifiers are compared with stored, fraud-related Phoneprints that Pindrop has collected into a blacklist. Similarly, Voiceprint classifiers are compared with stored, fraud-related Voiceprints in a corresponding blacklist. Along with comparing Phoneprinting and Pindrop Voiceprinting, the Protect solution reviews call metadata associated with the presented phone number for any fraud risk factors, including the identification of phone number spoofing risk or association with historical fraud identified in the Pindrop Fraud Consortium. The Phoneprint comparison, voice bio comparison, and the metadata analysis comprise the Risk Score.

The Risk Score is used in real-time to influence risk-based authentication and enrollment decisions on live calls. The Risk Score for a call is also used for the creation of a Fraud Case. Calls that meet the criteria specified in a policy rule are designated as Fraud Cases to be reviewed by a fraud analyst to determine whether the selected call as possible fraud was a genuine customer call or attempted fraud.

General Workflow (Authentication)
Phoneprinting for Authentication: Passport looks to match DTMF and codec audio characteristics (Toneprint) and artifacts to an enrolled caller device as part of the overall Phoneprint analysis for the purposes of matching the enrolled device.
Voice: As a caller speaks in any form with the IVR or agent, Pindrop Passport passively extracts voice features (not the content) and classifiers to output a unique voice feature for each caller. As the solution analyzes more calls for a specific caller, there is a maturation process designed to protect against degradation over time. The voice features are a sequence of floating point numbers and are non-reversable to speech. Pindrop analyzes the caller behavior of how a caller presses the keys on their phone for behavior matching for authentication. Pindrop pre-ring analysis for Caller ID Validation interrogates several conditions within call metadata for each call, analyzing anomalies in each call through metadata analysis to assess risk before the call even connects to its destination. A primary output of this pre-ring analysis is intelligence about whether the Caller ID is legitimate and if it can be trusted.

Presentation Attack Detection Capabilities
Received top ranks in the ASVSpoof 2017 and 2019 challenge on presentation attack detection track (aka replay attacks).

Synthetic Speech Detection Capabilities
Pindrop received top ranks in the ASVSpoof 2019 and 2021 challenge Logical Access (i.e. voice conversion and speech synthesis) and deepfake detection. Additionally, Pindrop's research has recently been quoted in major media publications such as WIRED magazine, where Pindrop correctly identified audio samples as human vs. synthesized (which were generated from Google's voice-synthesis technology called WaveNet).

Results of recent benchmarks
The benchmark studies are anonymous. The regulations of NIST, ASVSpoof prevent participants from publicly disclosing their rankings of performance metrics. However Pindrop continuously scores among the best on the NIST Speaker Recognition Evaluation (NIST SRE) benchmark and voice spoofing detection challenge (ASVSpoof).

Approach to tuning, calibration, and optimization
Pindrop solutions deployment involves the following steps:

- Solution need analysis – what problems need to be solved? authentication and/or fraud
- Assessments – business, telephony, and contact center reviews
- Integrations – implementing the Pindrop solution within a customer environment
- Training – knowledge transfer on how the Pindrop solutions operate and best-practices for authentication and/or fraud workflows
- TFN cutover – routing of customer toll free numbers through the Pindrop solution
- Production use – customer use of Pindrop solution in daily business operations
- The Pindrop APIs are the primary method to interface with the Pindrop solutions; to interface IVR transactions with Pindrop, for enrolling and authenticating callers and for querying for risk intelligence about a call. The core operations within Pindrop APIs include call control, account correlation, caller ID validation, enrollment, authentication feedback and risk management. The HTTP-based API is organized around REST and has predictable, resource-oriented URLs. When appropriate, JSON or XML is returned by all API responses.
- Tuning and calibration of machine learning engines to optimize fraud and authentication results is key. This process is undertaken continuously and involves following steps

Agent User Interface
Pindrop Passport and Protect have its own User Interface (UI) which is accessed via a web browser over HTTPS/TLS. This UI provides access to detailed call reporting that can be exported for use in external analytics engines. The UI contains web pages for dashboards, calls, cases, and policies.

Management Reporting and User Interface
Pindrop provides dashboards and reports for authentication, caller activity, fraud case load and several other custom reporting that provides real time telemetry and trends into each customer's authentication and fraud funnel.

Technology - Network Authentication and Fraud Detection

Device/Number Possession
SS7 data access: VeriCall gets the needed SS7 data in the SiP Invite Header. We don't require any sort of special SS7 access to access the data we need to perform the device/number validation
Carrier Partnerships: VeriCall does not need carrier partnerships to get access to carrier metadata. VeriCall is carrier agnostic and performs a direct inspection on the SIP header data for all calls.

Device or number based: VeriCall performs ANI validation to confirm a call is coming from the device that owns the number. VeriCall and Pindrop also perform network and geography mismatch assessments which contribute to an understanding of risk associated with the device and the caller ID.

Number/Device Reputation
Caller ID Validation analyzes the carrier signaling elements associated with an incoming call to look for missing or anomalous combinations of these elements that indicate call information was tampered with. This carrier-level signaling includes information about the call origination, call path, and call delivery. Additionally, Pindrop obtains the telephone number of the incoming caller from the Automatic Number Identification (ANI) or Caller Line Identification (CLI) information associated with that call and sends it to the Pindrop Intelligence Network (PIN) to query for aggregated risk factors from internal sources and the third-party carrier metadata service.

Carrier Partnerships for SIM/SWAP mitigation: Pindrop or Next Caller does not perform SIM Swap check

Own or third-party partnerships for number ownership validation
Pindrop or Next Caller does not own or have a third-party partnership for MNO data since both can deliver high ANI validation performance without needing MNO data. However MNO data can be integrated by organizations with either solution if required. ANI Validation confirms that a call is coming from the device that owns the telephone number.
Spoof detection determines when there is a high likelihood that the ANI has been manipulated by call spoofing.

Call Anomaly Detection Capabilities

- ANI velocity - Determines the risk of a call based on the frequency that a phone number has called into an organization in a rolling period of time. The risk factor does not monotonically increase as the frequency of calls increases, but rather there is a window where the risk increases, and then may decrease or drop off completely as the frequency continues to increase. The intuition for the risk factor is that fraudsters tend to call the contact center more frequently while building and executing attacks, although generally the risk output needs to be combined with other risk factors to reduce false positives
- ANI Reputation - Can raise or lower the risk score based on recent high risk or low risk calling behavior, respectively. The degree to which the reputation affects the risk score is a sliding spectrum and can change from positive to negative (and vice-versa) with each new call, although it tends to require multiple calls. The risk factor is useful in creating more separation in the risk scoring bands between genuine customers (the vast majority of callers) and fraudsters
- Carrier Risk - Determines the risk of a call based on the carrier associated with the calling ANI. This factor is aided largely by the confirmed fraud case labels that are collected in the Pindrop Consortium
- Consortium Risk - Determines the risk associated with a calling ANI based on the history of events for the ANI as captured in the Pindrop Consortium. Fraudsters may continue to use the same phone number to attack different organizations, especially within the same vertical
- ANI Blacklist - A list of phone numbers that, when matched to a call, will elevate the risk score significantly, regardless of low or high risk from other risk factors. It is best practice to review, modify, and purge the blacklist on a regular cadence

Approach to scoring, tuning and calibration
The call risk score comprises an intelligent ensemble of all aforementioned risk factors, including spoof detection, phone number metadata, carrier metadata, consortium risk, calling patterns, fraud voice, fraud device, and fraud behavior. The score is updated as new information is available. The fraud detection system is initially implemented with default parameters and weights for each risk factor and call risk score ensemble based on industry knowledge. An initial fraud alert policy is set that will create a case for any call above a given score, which is based on ROC curve assessment of fraud detection rate and false positive rate. As calls are captured and cases triaged by the fraud analyst team members, the system automatically adapts risk factor and scoring weights and parameters to increase the overall fraud detection rate and reduce the false positive rate.

Privacy protection mechanisms
VeriCall determines when an inbound call is coming from a device that owns the telephone number shown on the caller ID. Calls that cannot be validated, or in high-risk situations where the number is likely spoofed, businesses can take steps to protect customer information. This can include avoiding ANI match for the call (automatically connects an incoming phone number with an existing customer account to enable personalization and prediction engines or to step-down authentication for customers), limiting self-service options in the IVR, or even stepping-up authentication measures to enhance security.

Investigation and case management capabilities
Based on the policies configured by an organization, Protect will create a case for a call if the risk score exceeds a certain threshold. At this point, the call is only suspected of fraudulent activity and needs to be reviewed by an organization's fraud analyst to either confirm that the call is fraudulent or to determine that the call was from a genuine customer.
A fraud analyst typically starts an investigation that includes listening to call audio, comparing information from the call to other cross- channel information for the relevant customer or account.

Intelligent Authentication methods and principles
Pindrop offers a single, unified solution for intelligent authentication and fraud detection. The solution has two parts (i) Passport - for authentication and ii) Protect - for fraud detection and investigation. Pindrop also offers VeriCall for ANI validation and spoof detection. Following are the Intelligent Auth methods employed in each:

Passport

- Voice biometrics: Deep Neural Network (DNN) based, language / speech agnostic, text independent voice biometric engine Deep Voice 3.0. The voice engine passively analyzes a caller's voice as they naturally speak (no need to repeat fixed-phrases) and is resilient against channel artifacts and background noise. It works in the IVR and at agent leg. Deep Voice can enroll and authenticate callers with ultra-short utterances and sub second speech availability. Deep Voice is also designed to protect against degradation of voice prints over time.
- Carrier metadata: Passport analyzes carrier SIP header metadata to perform ANI validation. The ANI validation score along with risk and reputation analysis can be used to remove KBAs from an organization's authentication process
- Call risk: Passport uses Pindrop Intelligence Network which includes the Consortium and proprietary risk engines to assess risk on every call. The risk assessment allows organizations to validate callers especially ones with low-risk ANIs and remove KBA questions from the authentication process
- Behavior: Passport leverages DTMF keypress pattern analysis as well as call behavior data (ANI velocity, calling patterns) to separate genuine callers from potentially fraudulent callers
- Device: Passport leverages proprietary Phoneprinting technology to evaluate acoustic and contextual signals from calls to form a device profile that can be used for authentication

VeriCall

- Carrier metadata: VeriCall performs a carrier SIP header metadata assessment to evaluate risk level of the presented caller ID, which allows organizations to trust the ANI to remove KBA questions or other active requirements (like a PIN code or Member ID) from the authentication process
- Spoof detection: VeriCall also performs spoof detection on all calls to identify a multitude of spoofing methods and their associated risks related to level of trust that can be associated with the call and the number on the caller ID.
- Protect
- Voice biometrics: Deep Voice 3.0 leads the industry in presentation and replay attack detection as well as deepfake detection. Voice biometrics can also be leveraged to extract non-reversible voice prints that can be used to detect fraud by matching against known fraudster blacklists

IMPLEMENTATION

- **Delivery Model**: Both direct and channel. Direct delivery model based on Sales and Sales Engineering team supported by Business Advisory group. Channel sales based on partnership and technology integration with Verizon
- **Primary partners**: Dimension Data, British Telecom, Bell Canada, Telefonica, Twilio, Amazon Web Services, Aspect, Verizon, Speik, Avtex, Carahsoft, Genesys, Gigamon, Presidio, Transmit Security, Telnorm, Five9 and Intrado.
- Pindrop provides fully cloud based and on-prem solutions
- **Pricing**: Enterprise solutions: Tiered by call-volume (higher volumes reduces the price); IoT: by device, transaction or user
- R&D headcount 95
- Patents: 40 (US: 32, Foreign: 8 - Australia: 4, Canada: 3, Korea: 1). 80 applications

Vision & Plan
Fraud will continue to evolve in both volume and sophistication. Post Covid-19 contact centers have seen significant increase in fraudulent activity especially in the IVR. A large portion of fraud originates in the IVR in the form of account reconnaissance and then transpires in other channels or parts of the organization. Detecting fraud before it happens and taking precautionary measures in advance is the need of the future. Account risk monitoring and cross channel fraud prevention are critical areas for the future. Pindrop is investing in this trend by developing fraud alerting capabilities that would enable real time account risk monitoring and future mark and monitor strategies for cross channel fraud risk management.

Key Differentiators

- First time caller authentication: Passport and VeriCall can leverage a combination of carrier metadata assessment, call risk assessment, ANI reputation and spoof detection to validate first time calls without enrolled device or voice profiles.
- Secure enrollment: Relying on KBAs or legacy authentication methods exposes an organization to the risk of enrolling fraudster devices and voiceprints since they can bypass KBA questions at a high rate.
- Continuous and comprehensive fraud detection: Unlike legacy fraud detection tools Pindrop is not siloed and is active across all stages of the call in all parts of the call center.

Prove

Headquarters: New York City, New York, USA
Year business started: 2008
Investment/Funding: $198.8M Total, $98M Series H.
Revenue (estimate): $80M - $100M
Number of employees: 277

Overview
Prove's 'PRO' Model of Identity Verification & Authentication is the only model in the market that uses three checks to establish customer identity. These three checks, when used together, make identity fraud expensive and unscalable for fraudsters. As mentioned above, the "what you have" or "Possession" check is particularly effective in that it provides a binary answer to whether you are interacting with your customer or someone else. The person is either in possession of the associated physical device, or they are not.

The PRO Model: Possession, Reputation, and Ownership:

- Possession answers the question: Is this customer in possession of the phone number? Knowing that someone is in possession of a phone at the precise moment of a potential transaction helps identify someone regardless of the transaction channel and helps ensure the customer is truly on the other end of an interaction.
- Reputation answers the question: Are there risky changes or suspicious behaviors associated with the phone number? Typically, people have had the same phone number for a long time, and upgrade phones only every few years. Compare that to a burner phone, or a phone that underwent a SIM swap recently, or a phone number that was just registered. These activities lower the reputation of the phone itself, which allows companies to flag the phone regardless of the customer activity.
- Ownership answers the question: Is the customer associated with the phone number? It is crucial to associate a phone number to a person when confirming that the customer is in possession of the phone. Otherwise, the wrong person may be verified. This means knowing when a customer truly gets a new phone number or knowing that phone number is still associated with a person even if they switch carriers.

Prove's Phone Identity Network (PIN), which leverages the PRO Model to verify and authentication identities, is a registry of 1 billion+ identity tokens under continuous management. PIN is informed by multiple data sources including telecom, bank & public, and 10+ years of proprietary Prove data.

CAPABILITIES

Core Authentication
Text Dependent
SMS OTP, Instant Link

- Instant Link for Web: Allows the client to perform out-of-band authentication with a subscriber using an authentication link inside an SMS sent to the subscriber's mobile device (Active out-of-band authentication).
- Instant Link for Web can also be supported through the use of a QR-code instead of SMS delivery.
- SMS OTP: The SMS Delivery application sends a text message with a one-time code to the user's mobile phone number. The application delivers the one-time code via short message service (SMS) to be validated. The customer verification code generated during the web session performs the authentication if it matches the code sent to or generated by the MFA Platform for delivery by the SMS Delivery application.

Text Independent
Mobile Auth, PushAuth, GaitAuth, Behavioral Biometrics providing frictionless solutions identifying the person behind the device.

- Mobile Auth: Provides a real-time authentication of the status of a subscriber on a mobile network, thereby helping clients securely, instantly and silently authenticate a mobile number without sending an SMS OTP (Passive out-of-band authentication)
- Push Auth: Uses Prove mobile SDKs to deliver a notification on an individual's device prompting the user for an action. The SDK leverages device's signals and sensor readings for authentication and fraud prevention. The PushAuth solution can be used to securely authenticate an individual on a mobile device, as well as securely link browser sessions with trusted mobile devices.
- Gait Auth: Uses Prove mobile SDKs to learn an individual's manner of walking (an individual's "gait") and use that as a passive, behavioral biometric signal for authentication.

- PinDelivery: The PinDelivery application places a call to the end user and prompts them through a series of keypad entry sequences. The application delivers a one-time pin to the end user for entry into a corresponding web session. Validation of the one-time pin is performed by the customer's infrastructure
- PhoneConfirm: The PhoneConfirm application places a call to the end user and prompts them through a series of keypad entry sequences. The application is intended to authenticate the user's web session by confirming a locally visible confirmation number on the web session that the user matches on the call either verbally or via keypad entry.

Short Utterance Text Independent Authentication (Voice Biometric & Voice OTP)
The BioCapture application places a call to the user and prompts them through a series of voice recording sequences. This application enrolls the end user by creating a voice print ID (VID) for later use.

BioVerify: The BioVerify application places a call to the end user and searches the server for the user's voice print which was filed during the BioCapture enrollment process. Based on the user's voice print ID (VID) as collected during enrollment, the application verifies the user's identity by matching the spoken confirmation number against the existing voice print.

Fraud Detection for MFA (For Voice Biometrics OTP):

- Prove OTP block list: Prove's MFA platform keeps a customer defined list of blocked fraudulent phone numbers and fraud centric country list to prevent fraud before occurring.
- Voice Scoring: Prove uses voice recognition in its voice biometrics solution comparing the verification step with a prior enrollment. Each voice print is scored against prior enrollment preventing fraud. Prove sends a final status for misdiagnosed voice print

Fraud Detection
The Prove Identity solution comprised of TrustScore + Identity Verify APIs provides a solution for Risk & Fraud Identity verification includes verifying consumer's identity (Name, Address, SSN, Birth Date) and satisfying compliance with KYC/CIP with GLBA data sources:

- Phone ownership verification (Identity Verify) and phone reputation (Trust Score) leveraging real-time phone intelligence and ownership data
- Standardized settings help clients implement out-of-the-box and maximize verification rates while mitigating common types of attacks
- The Trust Score is routinely tuned against fraud feedback keeping clients protected from attacks
- Customer Success professionals work with clients to report metrics and work with clients to optimize their use of Prove

Technology - Network Authentication and Fraud Detection

Device/Number Possession
Prove's telephony network capabilities, collectively called Mobile Auth, are built on Carrier partnerships, leveraging the encrypted authentication of a device onto the carrier network to verify possession of a specific phone number on the device.

Carrier Partnerships:

- US - Verizon, AT&T, T-Mobile
- Canada - Bell, Rodgers, Telus
- UK - EE, O2, Vodafone, Three

Device or number based
Mobile network-based, using the mobile number to verify with the carrier that traffic is actually coming from the expected device and phone number.

Number/Device Reputation
Prove's proprietary algorithm consumes carrier signals and uses Prove's managed identity intelligence to generate a Trust Score™ for the phone number. Signals include the frequency, tenure, and recency of phone changes (e.g., SIM swaps, ports, phone number changes, device upgrades), and other carrier and internal phone intelligence. The Trust Score™ algorithm was developed with 10+ years of phone intelligence data and is continuously enhanced based on feedback and fraud trends. Although not required, Prove can access additional real-time signals from the Mobile Network Operators (MNOs) that improve the precision of Trust Score™ with consumer consent.

Call Anomaly Detection
Prove OTP Velocity Blocking: Prove places velocity limits on transactions to specific numbers and blocks of numbers to prevent fraudulent activity such as IRSF. Velocity limitations are informed via historical usage rates and are placed in effect by country and number block.

Fraud Mitigation and Methods

- Synthetic Identity detection with Identity Verify
- Account takeover prevention with identification of port attacks and sim swaps
- Burner phone detection with identification of short tenure and high velocity of change events. A burner phone is when a bad actor uses a phone for fraud for a short period of time and then disposes of the phone.
- Recycled phone detection when phone disconnects are identified in conjunction with a new user of a phone. A recycled phone number is the reuse of phone numbers formerly belonging to consumers.
- Social Engineering detection with geolocation detection and contextual authentication.

Technology - Behavioral Biometrics

User Authentication
Prove's Behavioral Biometrics Suite takes a mobile-first technology approach to leverage the signal readings from a smartphone's sensor to build behavioral models to identify and authenticate the person behind the device.
Prove's Behavioral Biometrics Suite is ideal for authentication of registered users coming back to the application of interest, working on the engagement process beyond enrollment. Prove's GaitAuth leverages the motion sensors on a smartphone to uniquely authenticate a person based on the way they move and walk, providing a differentiated, frictionless, passive authentication experience for the end user without even having to take the phone out of their pocket. Prove's PushAuth product send a Push Notification to the app on the device and, once the user answers the notification prompt, that reply gets shared with additional contextual and environmental signals that can help determine the legitimacy of an activity. While these technologies are mobile SDK based, they can be used cross-channel via a hybrid approach: If a user is trying to log into an application on a desktop web experience, the log in can ping the mobile app on the user's mobile device to continue the 2FA / MFA authentication process leveraging the mobile sensor readings in that authentication flow.

Device Authentication
Device signals leveraged in Prove's behavioral biometric models for device authentication: Token, secure element, device changes, support on-device traditional biometrics

Fraud Detection
The unique differentiator of Prove's behavioral biometrics, as compared to other behavioral biometric vendors, is that Prove's Behavioral Biometrics suite is mobile based and runs in the background, providing signals that are not only good for fraud detection as part of a risk score, but also good for authentication. That said, all the mobile signals captured by the Prove SDK can be leverage into a risk score for fraud detection.

Integration Methods
Prove's Behavioral Biometrics SDK is available for both iOS and Android. Size is approximately ~2MB and there are different modules that can be installed depending on the use cases, from PushAuth to GaitAuth to other contextual and environmental signals of interest. Latest benchmarks show that Prove's Behavioral Biometrics suite is as accurate as a physical fingerprint for authentication, with 1/50,000 false-positive rate.

Approach to scoring, tuning and calibration
Typical implementation path involves embedded the Prove Behavioral Biometrics SDK into the target mobile application, which usually takes a couple weeks at most. The SDK will run in the background for about a week collecting device sensor readings to build a behavioral model of the end user. Once the model is built, the application can authenticate against that model, making the model-based authentication the main factor in a 2FA / MFA authentication flow. If for any reason there are doubts about the person behind the device when authenticating against the model, the MFA flow can fallback to more traditional factors such as a push notification or SMS OTP as needed.

Privacy protection mechanisms
The solution is being implemented not only in the US but also in Europe, compliant with all privacy regulations in the countries and regions where the solutions are being implemented.

IMPLEMENTATION

- **Delivery Model:** Both direct and channel; Throughout the implementation period and beginning on day 1, Prove will provide guidance, expertise, a data flow diagram to illustrate proposed service orchestration, and a proposed schedule for integration.
- **Partners:** Prove works with over 1,000 customers around the globe, many of them financial institutions and Fintechs, including 9 out of the top 10 U.S. Banks.
- Prove's US production environment is highly stable and secure with strong quality controls. Prove's production servers and network are hosted at top-tier, global data centers. The primary data center is in Denver, CO, and the backup facility is in Brookwood, OR. The data centers are designed to support mission-critical operations and provide industry-leading capabilities in physical security, power availability and infrastructure. Additionally, Prove's MFA platform which supports SMS OTP and Voice Biometric solutions is AWS Cloud.

- The Prove Professional Services mimics the standard implementation services but provides a dedicated team of 3-4 resources that will manage the project from start to finish and be available on the clients schedule and less dependent on individual Prove team/organization schedules. Professional Services allows for the customer to optimize the delivery schedule based upon their needs and operating rhythm. Prove will provide tailored support, training, and engagement.
- **Pricing:** Customers are offered Professional Services Units to purchase from Prove. Each Professional Services Unit equates to 40 hours of work irrespective of the work performed. Prove Professional Services Team will keep a track of hours worked in a time management system (i.e., QuickBooks) and provide Monthly Reports to customers detailing work performed against the agreed upon Statement of Work Global proprietary phone identity network streamlines customer acquisition and frictionless servicing.

Key Differentiators:

- Started on mobile, unlike most competitors who started on desktop/browser and can leverage environmental and contextual signals in ways others cannot.
- Only solution on the market that runs in the background (e.g., app closed, device locked, etc.) and works without the mobile app being open (not just in-session)
- Only solution on the market that can authenticate the person behind the device, not just address risk & fraud use cases.

SESTEK

Headquarters: Istanbul/Turkey
Year business started:2000
Investment/Funding: None
Revenue: N/A
Number of employees (directly related to IAuth): 15

CAPABILITIES

Technology - Voice Biometrics
Sestek voice biometrics provide **both** text dependent and independent solutions. Users can either be authenticated in real time using free speech; or users can be authenticated by repeating previously defined passphrases.

Minimum Authentication Net Speech Requirement
Requirement for authentication is 3 seconds, but it is flexible and can be altered according to client needs.

Minimum Enrollment Net Speech Requirement
For the enrollment, need at least 10 seconds voice data but it is flexible and can be altered according to client needs.

Fraud Detection
Watchlist
Provide Blacklist identification product recommended for max 200 unique voiceprints for best performance. More the voiceprint number, higher the risk of false alarms.

Cross matching
Forensic voice authentication product can perform many to many comparisons against fraud.

Describe a typical workflow
Antifraud teams detect suspicious interactions in voice enabled channels (Call centers, IVR). These calls are examined and added into a tracking list so that records can be compared to these users with upcoming calls.

Presentation Attack Detection Capabilities
System can detect recurring identical voice samples as presentation attack, rejects submission and label it as fraud.

Synthetic Speech Detection Capabilities
- Can detect recordings with synthetic speech
- Liveness detections allow to evaluate upcoming calls' resource whether it is coming from live or digitally synthesized source

Approach to tuning, calibration, and optimization of end-user implementations
System has default configurations embedded in its configurations file. During production trials, these configurations can be optimized according to security expectations of clients.

Management Reporting and User Interface
System can integrate with 3rd party reporting tools to represent collected data for analytics uses

Technology - Behavioral Biometrics
Sestek Biometrics work with orchestrator platform to integrate with speech-enabled channels like IVR and biometrics products to validate incoming user data such as phone number registered during enrollment process. FIDO client/authenticator authenticates users with their unique IDs.

Privacy protection mechanisms
- Sestek' s system security features as follows:
- Allowed and blocked IP addresses can be defined to allow clients will be able to make requests to the API. The service can be configured to
- Only accept requests if they are sent by IP addresses in the allowed list

- Reject requests if they are sent by IP addresses in the blocked IP list
- The services can be provided via HTTPS.
- The services can be customized to be used only by provided service user.
- All speech samples for all processes are archived. The API provides a method for deleting user archives.
- Voice Biometrics activities can be visualized on reporting interface as user based and transaction based.
- Reporting interface has authorizations to be granted for Ad users only. Additional attributes of AD users can also be used as authorization filters of reporting interface. Manual user creation is not supported.
- The voice prints, speech samples and configuration files in the storage can be encrypted with by using the AES 256-bit symmetric key.
- FIDO UAF client/authenticator for Android certified as L1 security level

Intelligent Authentication Methods and Principles
As a first layer of our voice biometrics solution, the technology processes voice data to create voice prints and make authentications of these voice prints. In second layer, collected data is used to adjust authentication results to business needs of client. For example, intelligent decisions such as user account lockdown, self-update of voice prints. In final layer, Sestek benefits from a conversational AI component orchestrator as a management platform and 3rd party integrator to verify user claims beside voiceprints.

Details:
The solution integrates with customer IVR or mobile app in order to receive API usage & voice data. It provides an API that enables control over the verification processes as well as querying capabilities. A user can be enrolled to the system, and then could be authenticated with related methods. A reporting interface is provided to view past operations, current voiceprint status of users and system statistics.
Roles of the Components:
- Biometrics Server: Performs the voice biometrics operations on voice data.
- Biometrics Database: Stores voice print info and metadata.
- Biometrics Storage: Stores voice prints.
- Reporting Interface: Displays biometrics activities and statistics.

All disk and database connections are made using the .NET Framework, which supports secure connections.

System Features:
Several controls are applied on voice samples, which are noise detection, speech recognition, voice change, and fraud controls.
- Noise detection: Noise detection is applied on each speech sample of the customer to determine if the sample is applicable for verification.
- Voice change: Compares a current speech sample of the customer with previous samples on the same call to determine if the speaker has changed. This feature can be treated as a fraud control as per configuration.
- Speech recognition: Confirms the current speech sample if contains the passphrase

These three above are considered as “bad content”, and there is an auto-cancel configuration to cancel an ongoing process when there are too many bad content samples. On the other hand, if a sample fails any fraud detection control, then the ongoing process is immediately cancelled. The services can be deployed in a distributed architecture to achieve scalability and redundancy. Supported mono audio formats are 8 kHz 16-bit PCM, 8 kHz Mulaw and 8 kHz Alaw. There is an alarm mechanism that can produce alarms if there are errors related to licensing or system faults (e.g. database access error, disk I/O error, etc.).

Enrollment Features
There are two configurable thresholds for enrollment operations:
- Ready to enroll: When a pre-configured amount of speech is stored, an enrollment process’ status is changed to ready to enroll. After this, commit method can be called on this enrollment process to create a voice print.
- Auto commit: When a pre-configured amount of speech is stored, an enrollment process can be committed automatically.

Authentication Features
Authentication processes can be configured to restart the authentication process after a rejection.

IMPLEMENTATION

Delivery Model: For local market (Turkey), sell direct. For international markets, through technology partners (voice infrastructure providers like IVR providers or telephony infrastructure providers)
Primary partners: NCR, CCR, IST Networks
Services Model: Private cloud, on-premise, managed service
Pricing: 3 models based on customer enrollment volume or number of agent seats or total of annual transactions.

IAuth intellectual property: 3 patents and 1 utility model. 6 full-time R&D engineers.

Vision & Plan
Sestek roadmap is to achieve a vision that includes API development for enhancement purposes and implementing potential fraud detection (gray list) feature for 2021-2022. More accuracy with less voice data. Behavioral biometrics studies become advanced. Sestek plans to become a complementary authentication factor of different security layers of the service system.

Key Differentiators:

- Biometrics solutions can be both provided as core technology or as an improving platform by with bundle of Sestek products
- Flexibility for unique business flows
- Highly skilled research and engineering team which combines academical knowledge and industrial experience

Smartnumbers

Headquarters: London
Year business started: 1999
Year IAuth market contribution started: 2017
Investment/Funding: Privately owned
Revenue: N/A
Number of employees (directly related to IAuth): 80

CAPABILITIES

Technology - Network Authentication and Fraud Detection

SS7 data access
PSTN access in UK as an OFCOM-regulated network provider, granting us access to privileged signaling information

Carrier Partnerships
UK via BT; working with BT to integrate with their Global Inbound SIP platform; also partnership with Verizon

Device or number based: Currently number based; future third-party integrations provide options for device-based authentication

Approach to number/device reputation

- Smartnumbers Protect uses a range of inputs to determine a caller's reputation and score:
- Smartnumbers uses multiple machine learning models to analyze more than 200 features of the call signaling.
- Smartnumbers takes into account the full caller history - even if the caller is trying to hide their identity such as withholding their presentation number or spoofing their caller ID.
- Smartnumbers provides proactive real-time defense from known fraudsters. Customers share information about confirmed fraudsters, instantly protecting other Smartnumbers users from the same fraudster, even if they have withheld or spoofed their number.

A series of static rules, showing whether a phone number is spoofed, withheld, international, a known fraudster, or whether the call is displaying malicious signaling patterns indicative of fraudulent activity.

Carrier Partnerships for SIM/SWAP mitigation
A probabilistic model analyses changes in call signaling that may indicate changes in device, location or network that may be indicative of a SIM swap.

Own or third-party
Actively working with partners in the UK and US to develop integrations with carriers that will give a deterministic answer to whether a number has recently been SIM swapped.

Call Anomaly Detection
Detection Capabilities
As outlined above, Smartnumbers Protect uses a combination of machine learning, domain knowledge and static rules for call anomaly detection. This is reflected in the risk score assigned to each call.

Approach to scoring, tuning and calibration
When analyzing a call, Smartnumbers Protect gives each call a score from 0 to 0.9 in increments of 0.1 - a higher score means a call is riskier and a score over 0.5 is deemed "high risk". Alongside this score, there are a series of "risk markers" which show if a call is withheld, spoofed, a known fraudster etc. There are two areas of machine learning models within Smartnumbers Protect - one model focused on fraud and the other on authentication.

From day one, an industry-standard fraud model will be active alongside real-time protection from known fraudsters in the Smartnumbers Fraud Consortium. Over a ramp-up period of 2-3 months (depending on the customer and feedback data received) sufficient data is gathered to move the customer to a model specifically tuned to their traffic and fraudster profile.

The authentication model requires a ramp-up period of 1-2 months (again depending on the customer and feedback data received) before the model is deployed on the customer's estate. Due to variation in organizations' voice network and the potential impact on customers, a generic model will not be deployed on day one. Once these models are alive, model updates are deployed on an agreed frequency with the customer, typically quarterly or biannually. Additional off-cycle model tunings or developments can take place as necessary and are chargeable, although some may be included as part of the contract.

Privacy protection mechanisms
Smartnumbers use strong sign-in mechanisms with multi-factor authentication. Access to data is audited. Access is also role-based and granted on a least-privilege basis.

- All data is encrypted in transit using TLS 1.2.
- Smartnumbers is accredited to ISO 9001 for all aspects of Quality Management and is ISO 27001 and IASME Cyber Essentials Certified.

Smartnumbers complies with data privacy regulation even in heavily regulated geographies. For example, Smartnumbers investigation/case management tools provide fraud professionals the ability to examine the full history of calls made by an individual, even if they have withheld or spoofed their phone number. However, in the UK usage of this capability is restricted to the investigation of fraud in order to comply with PECR & GDPR, protecting the privacy of legitimate callers.

Investigation and case management capabilities
Smartnumbers provides tools to help organizations to identify, investigate and prevent unknown fraud. Typically this is used by fraud teams for a number of key purposes:

- Identify calls with a high risk of fraud immediately after they have taken place so that they can be investigated quickly
- Manage potential confirmed cases of fraud effectively and efficiently between fraud team members
- Investigate the behavior and scale of fraudsters even if they have attempted to mask their identity by withholding or spoofing their phone number. This gives teams insight into the wider impact of an individual fraudster, and highlights calls that were missed by other fraud systems.
- Prevent recurrence of similar fraud and strengthen fraud defenses by sending feedback data into machine learning models.

Agent User Interface

- Customers can consume the Smartnumbers API so they can combine the Smartnumbers risk score with other indicators from other systems such as voice biometrics to provide a combined notification such as a screen pop-up.
- Customers can ingest the Smartnumbers risk score as part of their online fraud detection solution to provide a holistic indication of the total risk of a transaction.
- Customers could configure their contact center infrastructure to consume the Smartnumbers risk score and play a call whisper to notify agents to high-risk calls

Management Reporting and User Interface
Smartnumbers flag potentially fraudulent calls, and provide customers with reports to show why they are high risk.
Reports show details on suspicious characteristics and geographic sources of calls. This enables customers to identify trends and changes in fraudulent behavior, for example:

- The number of calls received and the number of high-risk calls.
- Visual representations of the volume, type and the country of origin of suspicious calls.
- Carrier level call meta-data and risk indicators for every call.

IMPLEMENTATION

- Delivery Model: Channel
- Partners: Nuance, Verizon Cisco, Genesys
- Secure, tenanted public cloud
- Pricing: Two models, channel-based and per call. Channel-based pricing is calculated as the peak number of channels the customer requires at peak time. Transactional-based pricing is charged per inbound call. Charged at an annual commitment, price decreases as volume increases.

Key Differentiators:

- Global solution: Smartnumbers offers a choice of integration interfaces to provide flexibility of deployment options to fit existing infrastructure and regional differences.
- Smartnumbers consortium: Native cloud-based solution provides real-time protection against confirmed fraudsters identified by other customers.
- Uniquely positioned in the UK: Ability to examine privileged call signaling analysis controlled by Ofcom provides visibility into withheld and spoofed calls in the UK which is not offered by any other vendor.

Spitch

Headquarters: Zurich
Year business started: 2014
Investment/Funding: Series A of €5m
Revenue: N/A
Number of employees (directly related to IAuth): 58

CAPABILITIES

Technology - Voice Biometrics

Short Utterance Text Independent Authentication
Spitch uses text-independent/free speech-based and hybrid (VB + one-off phrases and STT) cross channel voice biometrics approach with continuous authentication, speaker change detection, behavioral, emotional and semantic statistical models, and voice identification. Spitch engine also has text-dependent VB capability. Spitch proprietary engine also serves as part of anti-spoofing techniques, in case of text dependent verification.

- DNN modelling allows building language independent, but phonetically aware models that can be used in either text-independent, text-dependent or hybrid approaches. Neural network embedding architecture is used to learn voice biometric features (512 in total). X-Vectors are extracted from embedding layers of the network. The training data augmentation with noises and reverberation improves the performance of the embedding architecture. The embeddings outperform traditional i-vectors for short and long speech segments.
- Bottleneck features approach guarantees extraction of all biometric-related features
- Where required, Spitch fuses VB with face recognition to fulfil specific customer's needs. Spitch works also with partners that add complementary biometric technologies.

Minimum Authentication Net Speech Requirement: 5-7 seconds
Minimum Enrollment Net Speech Requirement: 30-40 seconds

Fraud Detection
Describe a typical workflow
For the known fraudster voice recognition, the system administrator creates a separate database of fraudster voices, collects the known and suspected fraudster voiceprints there, and the front-end system sends the request to this database in identification mode with the voice sample from each and every call. If the solution returns "match" response with one of the voices stored in fraudster database, an alarm sign/signal goes off to the agent's or security officer desktop. The solution accuracy in identification mode does not depend on the database size. The solution uses deep learning algorithms (artificial neural networks) and capable of learning from the raw data on voice recognition, behavioral features as well as discrimination between noise and speech signal. For the unknown fraudsters, use real-time speech analytics solution based on Spitch's speech-to-text (STT) and NLU modules. In this case, need to train NLU modules for fraudsters speech patterns detection.

Synthetic Speech Detection Capabilities
Believe that the existing core VB engines technologies for preventing spoofing attacks are not suitable for production solutions. In practice "playback" is the most common and easiest attack type. Technology-wise the text-to-speech synthesis and voice conversion are still too complicated and incomplete to really be used by fraudsters. The only real prevention of spoofing attacks must be achieved by using anti-spoofing features in voice biometrics application:

- Passive verification applied to a live conversation -> the human agent is always able to distinguish between the actual voice and synthesized one.
- Active verification applied to human-machine communication - the key-phrase must be dynamic, and the spoken utterance has to be checked by speech recognition system.

Approach to tuning, calibration, and optimization
Spitch tunes FAR/FRR rates and confidence level threshold for each client/use case individually. The reason is that different user groups / customer segments / individual customers or types of inquiries (e.g. trading by telephone) requires different threshold values for the FAR and FRR. Spitch VB backend returns a confidence level for matching the voice in the call with the voiceprint stored.

Agent User Interface
Spitch provides continuous authentication, so that the agent can see the actual confidence level of the verification process as well as accumulated probability assessment during the entire conversation.

Reporting & Audit & Evaluation tools
Spitch Administrating terminal has an evaluation dashboard where the user can see FAR/FRR/EER parameters of the model calculated on the population of the archived calls. FAR/FRR curves depending on the threshold are also displayed. The user can change the threshold parameter and the results will be recalculated with the new threshold.

Decision Making Approach
Spitch VB backend returns a confidence level for matching the live voice in the call with the voiceprint stored. The decision on whether to consider the verification process successful or not is taken by the agent based on the confidence level returned and confidence threshold. The threshold of the integral confidence level for decision making may vary depending on the topic of the call. A computation of the threshold in the system depends on the speech duration used for verification procedure and on the value of the FAR or FRR rate set in the model. Usually, one model can be used for all the use cases with the different thresholds. For example, above 0.5 for providing information about balance but 0.7 for trading operations. The system can detect the use case automatically from ASR/NLU module or the agent can select the use case manually. Once the use case is selected, the widget will show whether the threshold for this use case was reached or not.

Intelligent Authentication methods and principles
Text-independent and hybrid voice biometrics products from Spitch use live spontaneous speech to identify and authenticate callers in a few seconds and ensure continuous identity verification throughout the conversation. Over 100 different parameters of voice are measured (512 max.), which allows the VB system to reliably differentiate even between voices of full twins. Continuous verification of identity throughout the conversation ensures that the caller remains authenticated at all times and transactions are secure. A combination of proprietary methods helps prevent fraud associated with identity theft and even scan digitized audio-archives for a more effective analysis of suspected fraud cases in real and near-real-time, as well as offline investigations. Summary of key features:

- Hybrid approach for very quick authentications with randomly generated passwords to thwart spoofing attacks.
- Phonetics-aware text independent verification. In addition to general characteristics of the voice coded in a voiceprint, the system detects individual pronunciation of phonemes and words using STT data.
- Cross channel approach to significantly increase enrolment process for faster time-to-market/deployment. Adapted PLDA (Probabilistic Linear Discriminant Analysis) algorithm used for modelling channel variability.
- Automatic fraud attempts detection and referral to fraud/security department.
- Voiceprints can be enrolled using conversations recordings with subsequent live updating.
- Spitch VB is part of the omnichannel conversational platform based on microservice architecture ensuring seamless integration with Speech Analytics and Virtual Assistants for fully automatic customer authentication in self-services.

IMPLEMENTATION

- **Delivery Model:** Primary direct on-premises installation for maximum security; Cloud/channel delivery is also possible.
- **Primary partners**: Swisscom, Abramo, AdNovum, Avaloq, Inventia, TCS, Luware, Nexteria, NTT Data, etc.
- Offer private cloud, hosted
- **Pricing**: Licenses, SaaS, pay as you go, revenue-sharing

Vision & Plan
Zero-effort and high-security authentication is likely to rely on free speech or hybrid voice biometrics as the most convenient and natural remote biometric authentication method in combination with device identification. Also consider the importance of automatic identification by voice for personalized customer service automation (e.g. in Spitch omnichannel conversational platform and virtual assistants), as well as behavioral and emotion detection/analysis alongside statistical semantic models. Spitch considers the use of voice biometrics features within speech analytics dashboard as one of the most promising directions of potential expansion of voice biometrics across the enterprise. This may help security and fraud prevention as well as sales increase by analyzing similar voices in conversations together with their content. Another promising area is the creation of platforms for some areas and\or industries in order to share voiceprints across enterprises and channels. Such platforms speed up enrolment and significantly reduce time-to-market.

Key Differentiators:
- Hybrid approach for very quick authentications with randomly generated passwords to thwart spoofing attacks.
- Phonetics-aware text independent verification. In addition to general characteristics of the voice coded in a voiceprint, the system detects individual pronunciation of phonemes and words using STT (meta)data.
- Cross channel approach to significantly increase enrolment process for faster time-to-market/deployment. Adapted PLDA (Probabilistic Linear Discriminant Analysis) algorithm used for modelling channel variability.

ThreatMark

Headquarters: Czech Republic
Year business started: 2015
Investment/Funding: Venture

CAPABILITIES

Technology - Behavioral Biometrics

User Authentication
For user authentication, ThreatMark uses a whole set of data extracted from the probes, starting with a detailed fingerprint (answering the question: is it the device we have seen before?). This is supported by capability to profile the user from the perspective of behavioral patterns (how long the session usually is, what day they access the application, from which country & IP & ISP and so on). This profiling is augmented with passive behavioral biometrics analyzing the clickstream, mouse movements and typing rhythms. Together, it creates a trustworthy set of data that can be used to validate user identity.

Device Authentication
Device fingerprinting is one of the key features of the AFS solution. To precisely identify returning devices, ThreatMark uses an exhausting set of device information extracted from the browser (web), reported by device OS (mobile) or calculated from primary features.

- For the web channel (web browser), gather resolution, browser, installed fonts, installed plugins, screen size, OS type and version, various frameworks types and versions (.NET), list of browser plugins (Flash, Java, Silverlight) including versions and more.

- On mobile endpoints approx. 150 parameters are checked, including simSerialNumber, wallpaperHash, macAddress, visibleNetworks, bluetoothPairedDevices, sensorResolution, IMEI, MEID etc. It is not only the fingerprinting itself that makes the system robust it is how the device's IDs are used. Employ our deep behavioral profiling to tell whether the currently accessing or logged-in devices are associated with legitimate users or fraudsters or have never been seen before. Based on shared device intelligence, able to identify problem devices across multiple sites.

Fraud Detection
The main idea of the system is to monitor in real-time user online banking sessions and score their every possible interaction within those sessions from the security perspective. To achieve this goal, we use our JS probe (for the web channel) and SDK (for the mobile channel) to collect more than 400 metrics used for 4 main purposes:

- Reliable device fingerprinting
- Device security/health check
- Anomalous payments detection
- Validating user identity

Last mentioned monitors data containing inputs from the mouse and keyboard and other data which defines the user biometry, his behavior and device, such as location, IP, time and date, navigation patterns, inputs from a gyroscope, GPS sensor, resolution of the screen and browser, installed fonts, installed apps, IMEI, installed plugins, screen size, OS type and version, various frameworks types and versions (.NET), list of browser plugins (Flash, Java, Silverlight).

Integration Methods
Solution uses our JS probe (for the web channel) and SDK (for the mobile channel – both iOS and Android)
The JS Probe loader is a single line of HTML code that has to be included in every monitored page. On every end-user device, the JS Probe is remotely loaded from the AFS Analytics server that sits on the bank's premises or in the bank's cloud. Therefore, a proxy pass (reversed proxy) has to be set up. The monitored mobile apps have to be rebuilt while including our SDK. As for Android, the application with bundled SDK increases up to 450 kB. For iOS, it increases up to 3000 kB. SDK also creates a cache in the device's storage ranging from 10-100 kB according to installed applications. There is also

recommended (but not mandatory) API integration of the AFS Solution with the bank's core banking system to utilize the full automation potential of the AFS.

Approach to scoring, tuning and calibration
The main idea of the system is to monitor in real-time user online banking sessions and score their every possible interaction within those sessions from the security perspective. To achieve this goal, we use our JS probe (for the web channel) and SDK (for the mobile channel). The monitored information is transferred from the JS probes and SDKs (that are active on the client devices that visit/utilize monitored web pages/mobile applications) in real-time to the central Analytics server. The Analytics server then applies state-of-the-art machine learning and artificial intelligence to evaluate an overall risk score (and, if any, a list of security-related detections) of individual user actions within the monitored web page/mobile app. The risk score with the detections is then sent back to the bank within an API response, which the bank initially initiated (e.g., by the core banking system or existing fraud detection system). After receiving the risk score with the detections, it then depends on the bank's policies, how to further deal with the situation – e.g., block the payment, escalate 2nd-factor authentication etc.
The sensitivity/strictness of the detection engine resulting in a more severe (less severe respectively) value of the risk score might be adjusted during the deployment and production if needed.

Priv**acy protection mechanisms**
Since most of ThreatMark clients are banks, there is a strong emphasis on different privacy legislations. Therefore, we regularly evaluate our Solution from that perspective to ensure those privacy legislation requirements are at their highest standards. As an example, let's mention the EU's GDPR or Turkish BDDK. As it is possible to deploy the Solution On-Cloud, we have chosen the AWS cloud provider to fulfill the highest security and privacy settings. The AWS provides a long list of internationally recognized certifications and accreditations, demonstrating compliance with rigorous international standards, such as ISO 27001 for technical measures, ISO 27017 for cloud security, ISO 27018 for cloud privacy, SOC 1, SOC 2 and SOC 3, PCI DSS Level 1, and EU-specific certifications such as BSI's Common Cloud Computing Controls Catalogue (C5) and ENS High. Recently, AWS also announced compliance with the CISPE Code of Conduct.

Describe a typical workflow
The solution allows fraud analysts to use the built-in Case management via a web-based admin console (AFS Panel). In the Rule engine (also built-in), it is possible to configure a trigger when a case should be generated. Once the case is generated, it is ready to be evaluated by the bank's fraud analyst. The available features of Case management are observing all case-related data (payments, detections,…); tracking its history, selecting a specific assignee; commenting on the case, resolving the case (FP, TP, TN, FN). It is also possible to use webhooks within the Case management. For example, if the state of the case changes, AFS will fire the webhook to notify the client.

Intelligent Authentication methods and principles
The main idea of the system is to monitor in real-time user online banking sessions and score their every possible interaction within those sessions from the security perspective. To achieve this goal, we use our JS probe (for the web channel) and SDK (for the mobile channel) to collect more than 400 metrics used for 4 main purposes. It is reliable device fingerprinting, device security/health check, anomalous payments detection and validating user identity. The most crucial monitored information includes inputs from the mouse and keyboard and other data which defines the user biometry, his behavior and device, such as location, IP, time and date, navigation patterns, inputs from a gyroscope, GPS sensor, resolution of the screen and browser, installed fonts, installed apps, IMEI, installed plugins, screen size, OS type and version, various frameworks types and versions (.NET), list of browser plugins (Flash, Java, Silverlight) including versions an much more.

IMPLEMENTATION

- Cloud-based deployment, alongside with on-prem; both the options are delivered as fully managed services.
- **Pricing**: Varies based on the number of active users (active user = user that makes an online banking login at least once a year.) Other essential factors are the following: number of user logins per minute; required data retention; a number of monitored web/mobile apps; scope of the necessary API integration; peak API calls number per minute; a number of deployed modules of the Solution (up to 3).

Vision & Plan
The ultimate vision for ThreatMark is to bring trust to the digital world. More specifically it means that we aim to ensure that trusted relationships between users and businesses in the online environment.

Key Differentiators:

- Stop the fraud by focusing on 3 distinct layers: advanced threat detection, digital identity verification through behavioral profiling and biometrics, and transaction analysis.
- Solution is built to provide value just through simple JS installation, without complex API integrations. Meaning that we can provide value and ensure fraud prevention in less than 2 weeks.
- Dedicated SOC center - a team that works non-stop to recognize and reverse-engineer current threats and use the intelligence to feed the Global Behavior Intelligence Network - a system that uses previous threats and behaviors to enable quick and continuous monitoring and prevention of current and future frauds.

ValidSoft

Headquarters: London & Connecticut
Year business started: Incorporated 2003, Management Buyout 2016.
Year IAuth market contribution started: 2009.
Investment/Funding: Successful Series A1 – A7 capital rounds closed 2016 – 2021.
Number of Employees: YE2021: 100+ FTEs

CAPABILITIES

ValidSoft offers its √IP® voice authentication platform, centered around voice biometric authentication. The solution is security-grade (suitable for high-value/high- risk transactions), due to our Precision Voice Biometrics™. The omni-channel nature of ValidSoft's authentication platform, means that enterprises can deploy a holistic, consistent, and excellent CX across all their secure engagement channels. The solution deployments apply Intelligent Authentication by applying customizable business logic, using contextual factors, enabling step-up authentication, and combining the latest voice fraud prevention techniques such as replay/synthetic detection.

Technology - Voice Biometrics

Text Dependent
Support phrases (3-4 words or approx. 0.5 – 1.5 seconds of speech is optimal), digits as well as precision text-dependent mode using random digits translated by an optional integrated ASR engine (can be included with phrase). TD engine also incorporates optional phrase assurance capability to ensure speakers are enrolling using the correct phrase for optimal quality. Also support normal band 8kHz for telephony and wide band 16kHz for digital channels. As well as 1:1 authentication our TD engine also supports 1:n identification using fixed or dynamic clusters of enrolled models. The solution is capable of deployment in any language, and we have five pre-tuned and optimized 'out of the box' (TD) phrases.

Minimum Authentication Net Speech Requirement:
Require 3 repeats of the biometric phrase which approximates to between 4 – 6 seconds of customer speech.

Minimum Enrollment Net Speech Requirement:
Require 3-4 words or approx. 0.5 – 1.5 seconds of speech to perform a robust authentication.

Text Independent
Support normal band 8kHz for telephony and wide band 16kHz for digital channels. Acceptable results can be achieved in approximately 2 to 3 seconds of speech (4 to 6 seconds elapsed) and we also support continuous passive authentication where we can detect a change of speaker within a conversation. Speaker diarization is also supported for mono audio streams. As well as 1:1 authentication, our TI engine also supports 1:n identification using fixed or dynamic clusters of enrolled models.

Minimum Authentication Net Speech Requirement:

- Applied passively in a Contact Center our minimum required speech for a robust authentication is between 2- 3 seconds but this can be optimized post deployment.
- Applied in a continuous passive authentication mode for Use Cases such as conversational commerce, we can process a minimum of 0.5 seconds of speech and add this to a continuous authentication model.

Minimum Enrollment Net Speech Requirement:

- Use cases applied passively in a Contact Center the minimum amount of conversational speech required is 3-6 seconds.

Fraud Detection
ValidSoft does not impose any restrictions on the size of the watchlist as this will be use-case driven. In addition, the company provides for multiple watchlists which can be processed simultaneously and also apply several techniques for the dynamic reduction of watchlists for improved accuracy at high volume. For accurate real-time identification, ValidSoft technology is capable of processing audio in excess of 60 x real- time and leverages the latest techniques in DNN embeddings and model clustering technology for high accuracy & fast scanning, to provide live ultra-performant identification services.

Cross matching
ValidSoft does not impose any restrictions on the size of the cross-matched lists as our service is designed for highly performant offline processing. Furthermore, we have multiple techniques for the dynamic reduction of candidate lists which leads to improved accuracy in use cases requiring large cross-matching scenarios.

Presentation Attack Detection Capabilities
To protect against fraud via replay or presentation attacks, the system analyses the audio in real-time to detect whether it is a recording. The process of recording and replaying introduces distortion to audio enabling our system to accurately identify recorded (and played-back) audio. Another technique is Identical Utterance Checking, where the VB engine checks previous authentications for being "too identical" to the one being analyzed. A third method is the application of liveness checking. This is where a random element must be spoken, such as randomly generated digits. The speaker must then not only be the right speaker but also speak the right and expected random element. By doing this, recording another person's static phrase or random phrase will not be sufficient to pass given the random nature of the challenge, notwithstanding our other inbuilt detection methods. This is known as Precision Voice Biometrics™. ValidSoft also has a number of proprietary / trade secret and/or patented/patent-pending methods for replay detection.

Synthetic Speech Detection Capabilities
To protect against synthetically (computer) generated voice (deepfakes), the system analyses the audio and checks for abnormal characteristics such as abnormal pitch patterns (voice presenting slightly robotic) or in the case of the more natural sounding artificial voices some abnormal constancies not found in normal speech. ValidSoft also has a number of proprietary / trade secret and/or patented/patent-pending methods for synthetic audio detection.

Results of recent benchmarks
ValidSoft has successfully participated in most major academic benchmarking evaluations (i.e. NIST, ASVSpoof, etc.), and have done so for many years. Furthermore, the performance of ValidSoft's biometric technology is constantly independently assessed by major Enterprises, Banks, Academia, etc. to confirm the caliber of our technology performance against competitors for benchmarking purposes. Both the academic and independent evaluations are performed over many languages and in varied conditions. ValidSoft is pleased to consistently be the leading performer and, in some cases, outperforming our closest competition by up to 10x in real-world conditions. Our performance "out of the box" consistently outperforms competitive offerings.

Approach to tuning, calibration, and optimization of end-user implementations
To ensure the voice biometric service is fully optimized to the conditions and scenarios of use (e.g. phrase, audio conditions, etc.), ValidSoft recommends (but does not necessarily require) a lightweight tuning and optimization phase to be undertaken during the In Service and Rollout phases. The exact steps performed are outlined in more detail in ValidSoft Biometric Optimization documentation. At a high-level, this process allows ValidSoft to systematically ensure the service is operating at an optimal point of performance based on the conditions and requirements agreed with the client.

Management Reporting and User Interface
The √IP® platform and √oiceID™ solutions provide a comprehensive Web-based reporting portal as standard.
The reporting portal provides several management and usage reports that provide detailed information about the performance of the system. The reports provide information on individual authentications through to specific system metrics giving an overall perspective on how the system, authentication and on-boarding functions are performing. All reports provide the capability to download the underlying data in CSV format. Additionally, the portal allows for all information to be extracted so custom reports can be generated by individual clients at their discretion and integrated with their own reporting environments if desire

Decision Making Approach
Decisions are based on rules and predefined (customizable) thresholds. We have thresholds for biometric score, replay detection score and deepfake detection score. Rules are typically based around ValidSoft's "grey zone" scoring and the subsequent contingency processing, e.g. request repeat, perform Out-of-Band ("OOB") challenge etc. as well as accuracy of digit challenges when using mathematical Precision Voice Biometrics™.

Integration
The ValidSoft √IP® platform offers a series of well-defined REST Web Services for integration with CRMs, Agent Portal and extraction of auditing and operational data, including the management of user enrolments and associated data.
Where audio acquisition (integration) is required, this can be achieved using several standard protocols and transport technologies, as follows:

- ValidSoft's service can expose itself as a SIP client so the audio acquisition can be established via SIP / (S)RT. Using the SIPREC transfer protocol. This is an extension to the SIP protocol for call recording, https://tools.ietf.org/html/rfc7866. It offers a very versatile way to "fork" the customer (calling party) audio to an external SIPREC service for storage or analysis. ValidSoft have a comprehensive SIPREC service that can receive the forked audio stream for biometric analysis. The status and outcome of the session(s) in progress can be retrieved via REST APIs and displayed into the Agent portal / desktop, either on demand or by callback
- At the audio gateway level, we can use UDP / TCP network port mirroring to fork the RTP (audio stream). To do this, we would require a Network Switch with port spanning and mirroring. From this we will collect the RTP and pass it to the stereo audio capture service. The stereo audio capture service will separate the customer audio stream and pass it to ValidSoft for Biometric analysis,
- Where integration into the IVR is concerned, generally we leverage existing IVR modules to capture the audio. This audio is then Base64 encoded and passed to the ValidSoft service through our REST APIs, VoiceXML callouts to REST / SOAP APIs
- The ValidSoft platform also provides a set of well-defined RESTful APIs should further channel integration be required, e.g. App, Web, etc.

Available authentication methods
The ValidSoft √IP® platform incorporates the voice biometric engine and provides multi-factor authentication through OOB using either SMS, telephony or other Push notifications for example through messaging platforms such as WhatsApp for Business, Telegram, Viber etc. This out of-band capability provides Transaction Integrity Verification for the detection of MitM and MitB attacks as well as strong authentication for lower risk transactions or access. Default (or Step-up) authentication is provided by the voice biometric capability which can be deployed as pure voice biometrics (TD phrase or TI free speech) or mathematical Precision Voice Biometrics™ through the inclusion of OOB delivered digits and ASR.

The voice biometric authentication process can itself use step-up authentication through OOB if, for example, a biometric score was deemed non-deterministic and therefore the "possession" factor was invoked. The voice biometrics engine can be deployed separately but when deployed as part of the MFA platform there is no additional charge for the √IP® platform functionality.

Available fraud detection methods
Fraud detection is provided principally with the voice biometric capability. The available techniques include real-time processing against watch lists, continuous authentication (detecting change of speaker), detection of replay (presentation) attempts and the detection of deepfake generated audio (Synthetic audio detection). We also support the concept of "grey zone" processing where a 'zone', determined by the customer with lower and upper thresholds, is deemed non- deterministic (and so invokes retry, OOB etc.) but below the lower threshold is considered a fraudulent attempt.

Case Management
The ValidSoft platform provides a series of well-defined APIs and event proposition endpoints to identify and delegate issues or discrepancies which may require further investigation, and these can be integrated with clients' existing operational (case management) systems. Service can propagate events or alerts to well-defined endpoints to ensure case management is properly handled but done is such a way as to minimize impact and training to existing support and case management services and operators.

Data Privacy Compliance
ValidSoft is the only cyber security identity assurance developer with four European Privacy Seals, endorsed by European Union regulatory authorities. ValidSoft's solutions have been designed from the ground up (with continuous iterative development and advice of world leading in-house and external cryptographic and data protection experts) to minimize data collection and processing techniques, and use the most sophisticated obfuscation, pseudonymization and randomization techniques to harden our solutions from a data protection and privacy perspective. ValidSoft's customers can be confident that when they deploy its voice-authentication solutions, they do so in full compliance with GDPR, CCPA/CPRP, BIPA and all similar privacy compliance regulatory frameworks worldwide.

Rule Management
The ValidSoft platform can be configured based on specific rules and logic via the rules user interfaces designed optimally for the specific Use case. ValidSoft works with the customer to ensure the rules and logic applied deliver both a successful authentication flow, but also deliver a secure and flexible outcome commensurate to the risk of the transaction being secured.

IMPLEMENTATION

- **Delivery Model:** ValidSoft is pursuing primarily a channel-partner go-to-market model, using existing Fortune500 direct clients as references. However, we also support both direct customer engagements and channels, including through CCaaS, CPaaS, UCaaS and IAM channel partners as well as resellers and distributorships. The choice is generally down to whether a client is implementing on their own platform or using a cloud-based hosted service.
- **Partners:** Five9, Talkdesk, Vonage, Okta, OneLogin, Duo, RCDevs, Ingenico, among others.
- ValidSoft offers both cloud (SaaS), on-premise, hybrid and on-device/edge- computing deployments. For cloud deployments we support a customer's own private cloud as well as providing our own managed service cloud based on Amazon Web Services, supporting multiple regions to ensure data sovereignty where required. Our environment is also containerized meaning our cloud offerings are service provider agnostic (AWS, Azure, Google etc.).
- ValidSoft prefers to work with partners (train the trainer) to deliver professional services. Nevertheless, for large bespoke and on-premise deployments, ValidSoft has an experienced professional services team to engage with a client's deployment teams.
- **Pricing**: ValidSoft supports a number of flexible pricing options including transactional, user-based, volume-based and agent-based for contact centers. Pricing is determined by both use-case and volume.
- ValidSoft's technology is proprietary and 100% owned, and the software platforms, biometric engines and speech algorithms are protected under copyright law and/or as commercial trade-secrets. We also have 16 patents granted, as well as numerous additional pending patents and new patent applications in train. We also have an extensive portfolio of registered and unregistered trademarks and our proprietary software is copyright protected. Approximately 60% of our employees are dedicated to R&D.

Vision & Plan
Current enterprise and consumer authentication methods are demonstrably broken and can no longer be relied upon to identify the individual conducting the transaction. Only biometrics can assert identity and only precision voice biometrics is mathematically accurate and precise enough to be able to assure the identity of the individual. This is because voice biometrics is uniquely two dimensional – voice and context.

We believe that 'proof-of-unique-human' solutions will be mission-critical to all forms of human-machine/service and interactions, in the private, commercial and public sphere now and in the future, and we firmly believe that voice-biometric authentication, and especially Precision Voice Biometrics® solves this challenge.

From a pure speech science point of view our plan is to continue to invest in R&D in advanced Signal Processing, AI, ML and DNN techniques to continue to achieve even faster, more accurate and adaptive voice biometric models and processing. However, whilst ValidSoft already supports omni-channel voice biometrics on the existing channels we recognize today such as contact center agents, IVRs, Web and Apps, our vision and plan are centered around the emergence of voice as the new User Interface and particularly as it pertains to voice commerce (vCommerce).

The keys, clicks and swipes of today are already being replaced by voice commands, such as on home speakers, in vehicles and through Intelligent Voice Assistants (IVAs) on any channel. Whilst these today are not necessarily centered around voice commerce applications and therefore are more about what is being said than who is saying it, voice commerce will create the requirement for absolute identity assurance of the speaker. Through tight integration with IVAs and Natural Language Understanding as well as short-duration text-independent authentication and identification, the spoken command will inherently be the identity assurance.

Key Differentiators:
- Most accurate commercial voice biometric solution: independently verified (by Fortune500 enterprises) in head-to-head comparisons with leading competitors.
- Full omni-channel voice authentication solution: with support for on-premise, cloud (private and public) and on-device/edge.
- Ease of use/consumption: provider of a multi-factor authentication platform providing workflow and logic where the biometric engine is an integrated component (which can also be made available as a standalone SDK for integration into other solutions or as an on-device solution).

Veridas

Headquarters: HQ in Pamplona (Spain)
Year business started: 2017
Investment/Funding: Joint venture between BBVA and das-Nano (recently increased investment capital)
Revenue: 10M€

CAPABILITIES

Technology - Voice Biometrics

Short Utterance Text Independent Authentication
Minimum Authentication Net Speech Requirement: 3s
Minimum Enrollment Net Speech Requirement: 3s

Fraud Detection
Presentation Attack Detection Capabilities: Passive Replay attack detection + Active alive challenge + authentication

Results of recent benchmarks
Currently on 7th position on NIST SRE CTS challenge (min_cost-based ranking) with an EER of 2.6%
Veridas was present at the ASVspoof2021 challenge, finishing in 9th position in the PA (Physical Access) category.
SdSV Challenge 2020 text-independent task: ranked 2nd in the single system and 3rd in the multi-system (link)
Approach to tuning, calibration, and optimization of end-user implementations Veridas' dasPeak solution includes different calibration sets for telephonic and microphone (lossless) audio scoring. It also allows the use of whatever working point (threshold) that better fits use case needs (only the score is returned instead of a hard decision).

IMPLEMENTATION

Delivery Model
Both direct and channel market approach: Veridas has a direct sales team in Europe as well as in Latin America and the United States, although, increasingly, its sales volume come from the strength of its partner channel, both platforms, integrators, and commercial partners/resellers. In the case of voice, the role of partners is fundamental. Our solution is a very valuable piece of technology that needs to be integrated into a complete end-customer solution. For this, Veridas has developed integrations in the main Contact Center platforms (e.g., Genesys, Avaya, Twilio, etc.) and in chatbot platforms or conversational assistants (e.g., Link Mobility, Everis, etc.) to facilitate and accelerate its implementation. Veridas has also developed strong commercial agreements with system integrators and international resellers.

Primary Partners
Contact Center platforms: Genesys, Avaya, Twilio, Talkdesk, Amazon Connect, Enghouse, Odigo, etc.
Chatbot/virtual assistants: Link Mobility, Everis, Cognigy, IBM, etc.
System integrators: Deloitte, Minsait, KPMG, Avantgarde, Evolutio, etc.
Commercial partners: Deutsche Telekom

Veridas offers its voice biometrics service through its VeriSaaS Cloud platform, mainly deployed in AWS infrastructure in two regions: the EU (Ireland & Frankfurt) and the US (Oregon & North Virginia). Veridas has also deployed its solution on Microsoft's cloud service, Azure, specifically in Amsterdam.\

Pricing: Develops two different models to better adapt to the use case and the different client needs:

- Price per validation (API call): considering a validation either a voice enrollment or an authentication (for end-customer cost purposes, it is the same). This model is ideal for contact center scenarios, where end-users do not usually make recurrent use of this service.
- **Price per user:** a certain number of end-users are contracted, getting unlimited validations for a year. This model is the most suitable for implementations in chatbots or virtual assistants since interactions per user are much more frequent, unlike in a contact center. Therefore, it is interesting to opt for a model related to the number of users and not the volume. Offer packs in both models, with a minimum duration of 1 year.

IAuth intellectual property: Currently have 8 patents filed, of which 5 are already

Vision & Plan

- Providing confidence in the digital age: SaaS (Software as a Service) company that offers solutions to verify the real identity of people in the digital space. Developing proprietary technologies for face biometrics, voice biometrics, and identity document verification. Solutions are modular and scalable, adapting to the needs of each client. We operate globally since 2017 in demanding sectors such as Banking, Insurance, Telecommunications, Mobility, or Public Administrations.
- Your identity, your security: Deep commitment to quality, regulation, and compliance, submitting our technologies to the highest international standards such as NIST for facial and voice biometric verification, proof of life according to ISO 30.107 iBeta level 1 PAD, ISO 27.001, National Security Scheme in information security systems, RGPD or CCPA in California.
- A global team with a local soul: Veridas is an international reality, with more than 100 customers in 14 different countries. A team of 150 highly qualified people, present in Europe, Latin America, and the United States, which draws from its roots in Navarra, Spain, where headquarters are located.

Key Differentiators

- True experts: 100% Veridas developed solutions (patents owned worldwide)
- Leading technologies: AI-powered world-class NIST, top #3 verified technologies
- Modular solutions: SaaS served APIs & SDKs to build different customer journeys

Voice Biometrics Group

Headquarters: Rochester, NY
Year business started: Aug 2009
Investment/Funding: 100% private
Revenue: N/A
Number of employees: 13

Overview
The VBG Platform is a complete, "deploy-anywhere" platform which contains: multiple ML and DNN/TDNN voice biometric engines, support for multiple fraudster watch lists, several forms of fraud and spoof detection, a consent management system, a user data request system (capable of serving GDPR and related data rights request), gender, channel, and emotion classifiers, adapters to Microsoft Speech Server, Microsoft Azure Cloud, and Google Cloud ASR services, custom audio signal preprocessors for conversion and quality control, a highly scalable request broker, multiple APIs (VXML, SOAP, REST, and Streaming Media), a highly scalable database, an administrative interface (Dashboard), a developer interface with online documentation and demos (Visual Demo Center), powerful ad-hoc reporting for all data, canned reports, threshold based alerting support with automated user disabling, full system logging, full data encryption in transit and at rest, etc.

CAPABILITIES

Technology – Voice Biometrics

Core Authentication
Text Dependent – The VBG Platform has voice biometric algorithms which support multiple text dependent / prompted use cases (random phrases, random text, static phases, static text).
Text Independent – The VBG Platform has voice biometric algorithms which support text independent / free speech / conversational use cases.

Short Utterance Text Independent Authentication
Minimum Authentication Net Speech Requirement – 1.5 to 2 seconds, depending on language and use case.
Minimum Enrollment Net Speech Requirement – 30 to 45 seconds, depending on language and use case.

Fraud Detection
Watchlist
The VBG Platform supports multiple watch lists per customer application. Combinations of available metadata tags, such as gender, geography, line of business, and other elements can be used to create separate watchlists, which in turn reduces the size of comparative sets. Obviously, the fewer members in the 1:N comparative set, the better. However, there is no specific "optimal" number for comparative set size, as the VBG Platform is fully parallel processing enabled.

Cross matching
The VBG Platform does not have a specific M:N function. Instead, we treat these tasks as a series of 1:N tasks (which is functionally equivalent).

Describe a typical workflow
There are many workflows and use cases to consider.

Presentation Attack Detection Capabilities
VBG has numerous anti-fraud measures employed within the VBG Platform. Much of these capabilities remain undocumented or very lightly documented for security reasons. However, we provide detection of recorded playback attacks, synthetic speech (TTS) attacks, and computer modified speech (voice conversion) attacks. We also have some configurable behavior triggers to shut-down unusual end user attempt patterns.

Results of recent benchmarks
VBG has not participated in any NIST studies to date. This year however, we decided to enter the 2021 ASV Spoof Challenge, and assigned a masters student from our lab to the task. For the DF task, achieved an 8th place finish. For the LA task, achieved a 15th place finish.

Approach to tuning, calibration, and optimization
To begin with, VBG has two separate classes of engine technologies – ML and DNN/TDNN. Relative to tuning customer deployments, we achieve the best results when we pair a language and use case together. For instance, "Latin American Spanish + RandomPIN™" or "English + Free Speech". Specific characteristics of how people speak a specific language can and do vary greatly as you move around globally. As an example, U.S. English speakers tend to speak differently from Canadian, British, African, Indian, Australian, and other areas/countries with English speakers.

One of the first things to determine are the required languages and use cases – and whether have extensive ML and/or DNN/TDNN models already built. If collecting data, we can rapidly build custom models using our ML technology and then quickly deploy them into production. Once the system collects enough data, can build DNN/TDNN models and migrate customers to these models. The Admin panel of Dashboard application has built-in facilities to run EER jobs, review statistics, set optimal operating points, etc. Able to migrate from one engine to another with a simple GUI, and zero downtime for clients (dynamic model upgrade system).

IMPLEMENTATION

- **Delivery Model**: VBG has both direct and partner-driven sales. The majority of VBG's end user deployments are sourced by partners (roughly 5:1 ratio). Note that VBG has NO resale partners – all partners embed our technology within their own products and services for resale to their end customers.

- **Partners**: Amazon Connect, Aspect (now Alvaria), Intrado, PlumVoice, Telnyx, and Twilio, among others.

- **Cloud-Based Services**: VBG has two "public" US-based managed hosting environments for use by clients. "Hard iron" datacenters are provided by LiquidWeb (in MI and AZ), while our "cloud" datacenters are provided by Microsoft Azure (multiple zones). VBG also has private client deployments in Google Cloud, IBM Cloud, Amazon EC2, and Alibaba. Currently being deployed into a FedRAMP facility and will go through a rigorous, year-long audit and certification process there. VBG deploys anywhere – yet all deployments have some amount of on-going VBG management and involvement.

- **Pricing**: VBG's primary offering for hosting customers is a standard subscription model (unit prices drop as higher commitments are made). For premise clients, have recently deprecated traditional licenses in favor of "hybrid pricing". This is a large monthly tiered subscription approach – several price levels are provided, each with unlimited usage. Pricing is based on needed functionality bundles and user counts.

Vision & Plan
VBG's mission is to provide the high-quality voice biometric functionality that our clients want, when and where they want it, in an easy to integrate and highly scalable manner, all at reasonable prices, and with exceptional support.

- Value: VBG remains a strong value play. All the core functionality of the largest providers, all the metrics, all the scientific discipline. Again, as a web services provider, stop short of agent applications/interfaces. Value is further provided with free trials, simpler and more affordable pricing approaches, easier integrations and deployments, and with "white glove" support and consultative services.
- Scale: The VBG Platform has been processing many millions of transactions a year for quite some time now. The scalability of our US hard-iron data center was tested in 2020 with the addition of a new client having 1MM transactions per month. In Q4 we're adding another new client having 75K transaction (calls) per day. And VBG-run data centers have had no downtime in many, many years.
- Plug-Ins: Continue to add adapters to the platforms our clients and partners want support for. For years have supported platforms like Aspect, Intrado, Twilio, and others for traditional IVR use cases. However, added media streaming capabilities when and where possible to support real-time bot and call center use cases.
- Research: Completely re-oriented company's research process and are making substantial, leading-edge progress in almost every aspect of the core. This aspect of business model continues to grow and evolve rapidly and has resulted in numerous platform improvements in the past 18 months.

Key Differentiators:

- Appeal to Integrators: VBG has an "Intel inside" business model that should be very appealing to integrators and those wishing to white label voice biometric services. A lot of thought, time, and effort has been put into this part of our business.
- Flexibility: While don't have a mobile SDK or chip build (not ruling either out in the future), can deploy platform in almost any conceivable environment. In just about every public cloud and many different private hard-iron and VM based data centers.
- Intelligent Stack: Have a lot of process automation built into platform – from fully contained IVR dialogs, to fraud detection logic for many common scenarios, to GUI-driven data collection, EER studies, tuning/optimization, and engine migration routines.

Verint

Headquarters: Melville, NY
Year business started: 1994
Year IAuth market contribution started: 2013
Investment/Funding: R&D 18% of revenue for fiscal year ended Jan 31, 2021; Apax $400 million global investment
Revenue : $1.29M Verint global revenue for fiscal year ended Jan 31, 2021 of which IAuth is part
Number of employees: 4500 Verint global employees

Verint Adaptive Fraud

Verint Adaptive Fraud™ is a contact center solution that is unique in the voice channel fraud detection and customer verification market and presents key advantages. Developed 7 years ago as a fraud solution specifically designed for Verint customers, it leverages Verint's long (15 years) experience implementing and operating SaaS-based IVRs in the largest interaction-based financial self-service applications in the US. To date, Verint has analyzed well over 1 billion calls a year and understand and can capture the activities and behaviors of both fraudsters and legitimate callers.

- Verint Adaptive Fraud can capture activities fraudsters perform in the IVR that are precursors to fraud attacks (e.g. validating, testing, probing, re-pinning, address changes, telephone number changes, etc.).
- Verint Adaptive Fraud also captures behaviors displayed by legitimate callers. This capability helps call center live agents extend higher degrees of service as they can be sure they are interfacing with a legitimate caller. The reduction in Average Handle Time (AHT) can be significant when agents are able to quickly ascertain that the caller is legitimate, reducing both Telco and IVR costs.

In late 2018, Adaptive Fraud become available for implementation on any IVR and this year, to the Verint partner community. Given the robust nature of the solution's ability to capture voice channel analytics in real time, the use cases are endless and advantageous to call center operations.

What is Verint Adaptive Fraud?

- A robust analytics solution that can drive higher adoption of voice channel self-service, better live agent efficiencies, voice channel automation and "best skill" agent routing
- SaaS voice channel analytics solution deployed to verify legitimate callers and detect and stop fraud in the IVR in real-time
- Solution that captures and scores characteristics from the phone call and combines with both historical and real time behavioral analysis in the IVR
- Ability to disposition in real-time the IVR caller based upon a threat risk-score (numeric and scaled low to high) and blacklists
- Ability to identify in real time, Accounts under Attack by fraudsters for quick disposition e.g. suspension of the account
- Robust analytics that can be leveraged with other channels (e.g. live agent, web and mobile channels)
- Integrated with any IVR via a simple API
- Implemented in 30-45 days and provides impact quickly (usually within weeks)

Why is it important?

- Call center managers are experiencing a 40%+ YoY increase in traffic to live agent pools that are understaffed and remote requiring the need to accurately:
- Reduce AHT of all callers
- Deflect fraudulent calls to agent pools skilled to interface with fraudsters
- Deflect calls from live agents by establishing more complex self-service abilities
- Automate more calls in the IVR and other channels without lowering CX
- Lower exposures of ATO fraud in the call center environment
- Protect non fraud skill agents from interfacing directly with fraudsters
- Share voice channel analytics with other complementary analytics solutions in their enterprise
- Provide a frictionless, passive environment to increase CX and brand loyalty

Carrier Partnerships: Verint works closely with Verizon, AT&T and Lumen Technologies to utilize critical carrier level data in our Threat Matrix algorithms.

Device or number based: Verint uses carrier meta data combined with multiple 3rd party data to validate the calling number and device. Adaptive Fraud utilizes a large variety of data to assess the reputation of an ANI including but not limited to:

- Is the number on a Verint blacklist?
- Verifies that the number is a valid number
- Verifies the number is actually in service
- Identifies recently ported numbers
- Identifies risky line types and carriers
- Monitors calling activity both in the Verint network and in our partner/vendor network
- Analyzes the number of merchants a number has interacted with in the last 90 days
- Analyzes the number of unique identity elements paired with a number in the last 90 days

Carrier Partnerships for SIM/SWAP mitigation: Although SIM swap fraud is an issue in some environments, our customers have not been impacted. Verint has identified potential partners if the need arises.

Detection Capabilities: Verint Adaptive Fraud analyzes each call for anomalies in caller behavior and carrier meta data. The Threat Matrix fraud engines analyzes numerous parameters in real-time and assigns a risk score to both the ANI and any account accessed during the call.

Approach to scoring, tuning and calibration: Adaptive Fraud provides a real-time risk score for every ANI and account accessed during a call. Scoring is based on both machine learning and rules-based algorithms. Scores are tuned based on real-time feedback from an agent or fraud analyst and through our monthly Insights sessions.

Privacy protection mechanisms: Verint Adaptive Fraud utilizes a secure credential-based framework to govern access and no sensitive data is ever used or disclosed in the system.

Investigation and case management capabilities: Verint Adaptive Fraud provides a web portal and several reports to provide a fraud analyst with the tools necessary to investigate suspicious activity. High scoring ANI threats as well as high risk accounts are clearly identified and marked for investigation. An analyst can move alerts during the investigation stage to track progress. Once the investigation is complete an analyst can disposition an ANI or an account to the proper status and the Threat Matrix engine will automatically adjust the score according to the feedback.

Agent User Interface: Verint Adaptive Fraud provides a web portal to provide management statistics and alerts/data for analysts to use during their investigations. Additionally, Verint provides best practice integration at the agent desktop to utilize a risk score for an individual call. Uses CTI, CRM or external applications such as Verint DPA to provide Agent screen pops that tell the agent what level of risk each call has so they can provide the correct level of authentication. This significantly reduces AHT.

Management Reporting and User Interface: Verint Adaptive Fraud provides both summary and detailed level reports on current threats within the IVR including both ANIs and accounts under attack. CLARITY Dashboard: Leveraged by the Partner's fraud analysts, provides Real-time fraud status, reports and rules-based alerts. Provides ANI and account-level visibility and forensics for the Partner's fraud CSRs along with Blacklist and Account Watchlist management.

Verint Adaptive Fraud Engine with proprietary THREAT MATRIX - Real-time analysis of numerous caller behaviors across multiple calls and programs. Used to identify and flag suspicious callers based on threat level score generated via proprietary algorithms powered by machine learning. Proprietary technology developed by Verint:

- Analyzes 100% of calls, in real-time, for dozens of caller behaviors, reputation and knowledge
- Leverages ANI, SIP Header and other meta data to establish caller markers for future threat scoring
- Highly effective detection of Account Takeover fraud
- Ensures threat score accuracy reducing false positives
- Adapts and responds to fraud pattern shifts

Rule Management: One of the most important aspects of Verint Adaptive Fraud is monthly or quarterly INSIGHTS Advisory Services, an interactive consulting session between Verint and Partner analysts that utilizes expertise in identifying fraudulent behavior in the IVR and shifting fraudster tactics. The outcome of the INSIGHTS session is a set of recommendations on changes to the IVR call flow as well as the Threat Matrix scoring metrics that both Verint and the customer agree will hinder the success of the fraudster in the application.

Verint Identity Authentication and Fraud Detection

Verint Identity Authentication and Fraud Detection is a powerful solution that leverages recorder-embedded voice biometrics to authenticate callers faster, more easily, and more securely than traditional methods of authentication, while providing high levels of accuracy. It can passively screen calls in the contact center against dynamically updated databases of customer and fraudster "voiceprints" — digital representations of a person's voice that are unique to each individual. Screening is performed in real time, without disrupting the customer experience for legitimate callers. By minimizing or removing the need for

authentication questions that often frustrate callers, the solution can help contact centers deliver a better customer experience. It can also help enhance security by deterring professional fraudsters, who often defeat security questions and passphrases using a combination of social engineering, personal data found online, and repeat calls.

Capabilities
Verint Identity Authentication and Fraud Detection is an identity analytics solution that uses voice biometrics to help you verify customers and detect fraudsters. The solution is available as a complete, fully integrated suite for end-to-end authentication and fraud detection in contact centers. Its functionality can also be licensed as discrete applications that address each of these areas independently:

- Verint Identity Authentication recognizes the unique vocal characteristics, or "voiceprint," of enrolled customers seconds into a live call, helping to reduce the number of security questions—and average handle times. It can help reduce contact center costs while improving the customer experience.
- Verint Fraud Detection uses voice biometrics to identify professional fraudsters on calls by storing a database of known fraudster voiceprints. Fraudsters can be detected even if they answer security questions and dupe agents. This can significantly increase fraud detection rates in your contact center.

Text Dependent: Verint's Self-Service (Text Dependent) solution is PBX/IVR/IVA independent with out of the box API for integration to mobile applications.

Text Independent: Verint Identity Authentication and Fraud Detection uses voice biometrics to verify callers in real time passively, without requiring a password to be spoken. This makes authentication faster, easier, and more secure than traditional authentication methods.

Describe a typical workflow: The IAFD solution uses voice biometrics to perform repeat fraud detection. When the business discovers a fraudulent call, using the Risk Management application they can create a voiceprint and add this to the watch list. This watchlist is then screened against all incoming calls and can be used to alert an agent of the risk and hand the call over to a fraud specialist who is trained to handle potential fraudsters. Verint Risk Management can be used by the fraud team to further review this call along with other fraud calls to help profile the fraudster and the audio can be used to enrich the voiceprint to assist with future detections.

Synthetic Speech Detection Capabilities: Today, Verint already supports the ability to detect and block fake audio attacks for active biometrics. Verint's Active Biometrics has proprietary Replay Attack Detection and Liveness Detection algorithms detect fake audio that has been spliced together from various sources; that combined with multiple Signal Quality Monitoring algorithms are used to identify non authentic voice.

Approach to tuning, calibration, and optimization of end-user implementations: It is best practice to have 2-3 voice prints taken over an extended period of time to normalize the individual print. Note, the solution will work with one initial voice print. The tuning is set by customizable rules as to when to add a new voice print to the current voice print account.

Approach to scoring, tuning and calibration: Self- Service Authentication is integrated with the customer PBX/IVR/IVA and is a Text Dependent enrollment. During enrollment a series of phrases or digits will be repeated by the enrollee to capture and build a voice print. This allows Verint's Self-Service Authentication to be extremely accurate when comparing a voice to the ones stored on file. It is suggested that the voice be re-recorded every two years to keep an accurate print on file.

Privacy protection mechanisms: Verint products will support local privacy legislation using business rules and configuration. Verint does not act as a consultant as to the legislation that should be followed or implemented. The customers legal department must review and advise as to rules that would need to be put in place. All voice print data, as well as any stored customer or agent audio, is encrypted and secured with FIPS 140-2 encryption key management.

Investigation and case management capabilities: All data can be shared to a central case management system for analysis with links back to the specific call under investigation.

Integration: Voice Biometric information can be integrated using Verint's large API library. Authentication and fraud related alerts can be sent to agent and supervisor desktops in real time as well as the ability to send historical information to 3rd party case management systems.

Case Management: Verint's Identity Analytics solution is embedded within its core contact center applications, empowering organizations to orchestrate authentication and fraud detection workflows that can channel suspected calls into analytics solutions for further analysis, create real-time alerts and provide post-call interaction reporting—all without additional development.

Implementation

- Delivery Model: Direct and indirect sales

- Partners: Sell through Verint's partner network; offer both private cloud and hosted. Architecturally the solution is 100% cloud and is hosted in AWS, resulting in low upfront investment and short implementation timeframes. The solution is easy to configure and results in simplified and highly competitive pricing (per IVR call/month).

- Pricing
    - Verint Adaptive Fraud: Set Up Implementation Fee (one time); Per Call Usage Charge (recurring); Insights Advisory Sessions (recurring Monthly, Quarter, Half Year, Year depending on customer and their fraud environment; API Scripting (Customer incurred charge, not billed by Verint); Professional Services (ongoing as required e.g. IVR Dispositions)
    - Verint Identity Auth: Both transaction- and licensed-based; varies by package, size, implementation model and other factors.

- IAuth intellectual property: Approximately 30 approved and pending patents for IP we developed around IAFD. The broader Verint suite, which IAFD integrates into for extended functionality, has over 550 patents. We are unable to share number of R&D employees. R&D is approx. 18% of revenue.

Vision & Plan

Verint's solutions capture and analyze billions of customer interactions worldwide with the mission to significantly improve the customer experience, increase operational efficiency, inspire employee engagement and increase security. At the center of this mission Verint has demonstrated the opportunity for voice biometrics to be used to create frictionless authentication and identify fraud in real-time. Indeed, with the shift to work-from-home, organizations are more interested than ever in fraud prevention and solutions that easily deploy in hybrid work environments.

Voice biometrics will continue to remain core to our strategy of creating exceptional customer interactions that protect customers and organizations from fraud. However, we are increasingly incorporating analysis of other metadata and behavioral data to further improve upon the mission. While those other factors and behaviors are extremely valuable in the analysis, by themselves they are all constantly subject to manipulation through different fraud attack vectors. As such, a layered approach will still be the key weighing attribute in the analysis of fraud and authentication for years to come.

Key Differentiators:

- Verint Fraud Portfolio: The portfolio is robust and provides mid-size to extremely large enterprises with layers of complementary biometric solutions that protect the full customer journey; Unique to other self-service layers of fraud protection, Verint Adaptive Fraud™ leverages real-time caller behavior analytics to score threat risk of the caller.
- Dual screening of calls for both identity authentication and fraud detection in a single solution and uniquely combines this with conversational indicators to provide enhanced security and agent guidance.
- Application of behavioral analytics within the IVR in real-time provide the ability to take special action based on an assessed threat level; Predictive fraud engine combines complex data mining with immediate call dispositioning within the IVR.

VoiceIt

Headquarters: Minneapolis, Minnesota
Year business started: 2005
Investment/Funding: Seed
Number of employees (directly related to IAuth): 5-10

Overview
VoiceIt has two independent solutions. Once is a SaaS Cloud Restful API. This solution has many use cases and edge cases. Typical intelligent Authentication methods are integrated as 1:1 verify or 1:N to identify and verify an individual via multimodal biometrics with intelligent liveness challenges and replay attack technologies. The second preview solution is a Text Independent technology. It's raw low-level API allows integration into any call center applications. Typical interfaces have been with Twilio Flex contact center products. As a new caller is talking to the agent, background recordings can be manually or automatically sent to the VoiceIt speaker validation system and compared against the user's last call and/or against pre-marked fraud recordings. They usually build out a green, yellow, red stoplight indicating to the agent how confident they are talking to the right person. This gives the agent a way to validate the caller more before moving forward in the call session.

CAPABILITIES

Technology - Voice Biometrics

- Text Dependent: The VoiceIt Voiceprint Portal provides voiceprint phrase management for our developers. They can manage all their voiceprint phrases based on 88 different content languages. There are even wild card type voiceprint phrases that have words of the voiceprint be dynamic (Text Independent). These voiceprints allow the developer to enroll users, verify users, or even do identification in a group of up to 50 users.
- Text Independent - VoiceIt has created a new Text Independent technology preview outside the scope of the current VoiceIt API 2

Short Utterance Text Independent Authentication

- Minimum Authentication Net Speech Requirement - The SIV3 recording file must be at between 1.5 seconds and 5 seconds long and with a minimum of 1.3 seconds of continuous human speech with max pause between phonetics of 500 milliseconds (no long pauses) in the recording. The SIV4 recording file must be between 500 milliseconds and 15.0 seconds with a minimum of 400 milliseconds of continuous human speech with max pause between phonetics of 1200ms (no long pauses) in the recording.
- Minimum Enrollment Net Speech Requirement - The SIV3 recording file must be at between 1.5 seconds and 5 seconds long and with a minimum of 1.3 seconds of continuous human speech with max pause between phonetics of 500 milliseconds (no long pauses) in the recording. The SIV4 recording file must be between 500 milliseconds and 15.0 seconds with a minimum of 400 milliseconds of continuous human speech with max pause between phonetics of 1200ms (no long pauses) in the recording.

Fraud Detection

Watchlist: Can match as many different recordings per call against known fraud recordings.

Cross matching: This can be accomplished by using the simple API in matrix calling algorithm.

Describe a typical workflow: Run current session recording against individual fraud recordings back-to-back.

Presentation Attack Detection Capabilities: Developed new Liveness Services in addition to our previous Liveness Challenges. These use Neural Nets and Fuzzy Logic sub systems.

Synthetic Speech Detection Capabilities: Spoofing against human enrollments.

Approach to tuning, calibration, and optimization: Provide Model Tuning to customers. Model Tuning takes a provided data set of unique users, and creates custom parameters that result in the lowest False Reject Rate (FRR) AND a 0% False Acceptance Rate (FAR) based on the provided data set.

IMPLEMENTATION

- Delivery Model: Direct and Technology Partners
- Primary partners: AutnHive, Sagess3, Twilio, Upwire, Vonage
- Cloud-based services: Cloud/SaaS Multi-Tenant Managed Service, Private Cloud, Kubernetes
- Pricing: Cloud Hosted (Multi-Tenant) is per API Call, Private Cloud and Kubernetes are Per User Licensing and Per Node/Instance Licensing
- IAuth intellectual property: Patent #: US009799338

Vision & Plan
Become the first biometric company to have cyber resilience on user credentials that will solve compliance and privacy policies worldwide.

Key Differentiators
- Ease of integration
- Performance
- Customer Service

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