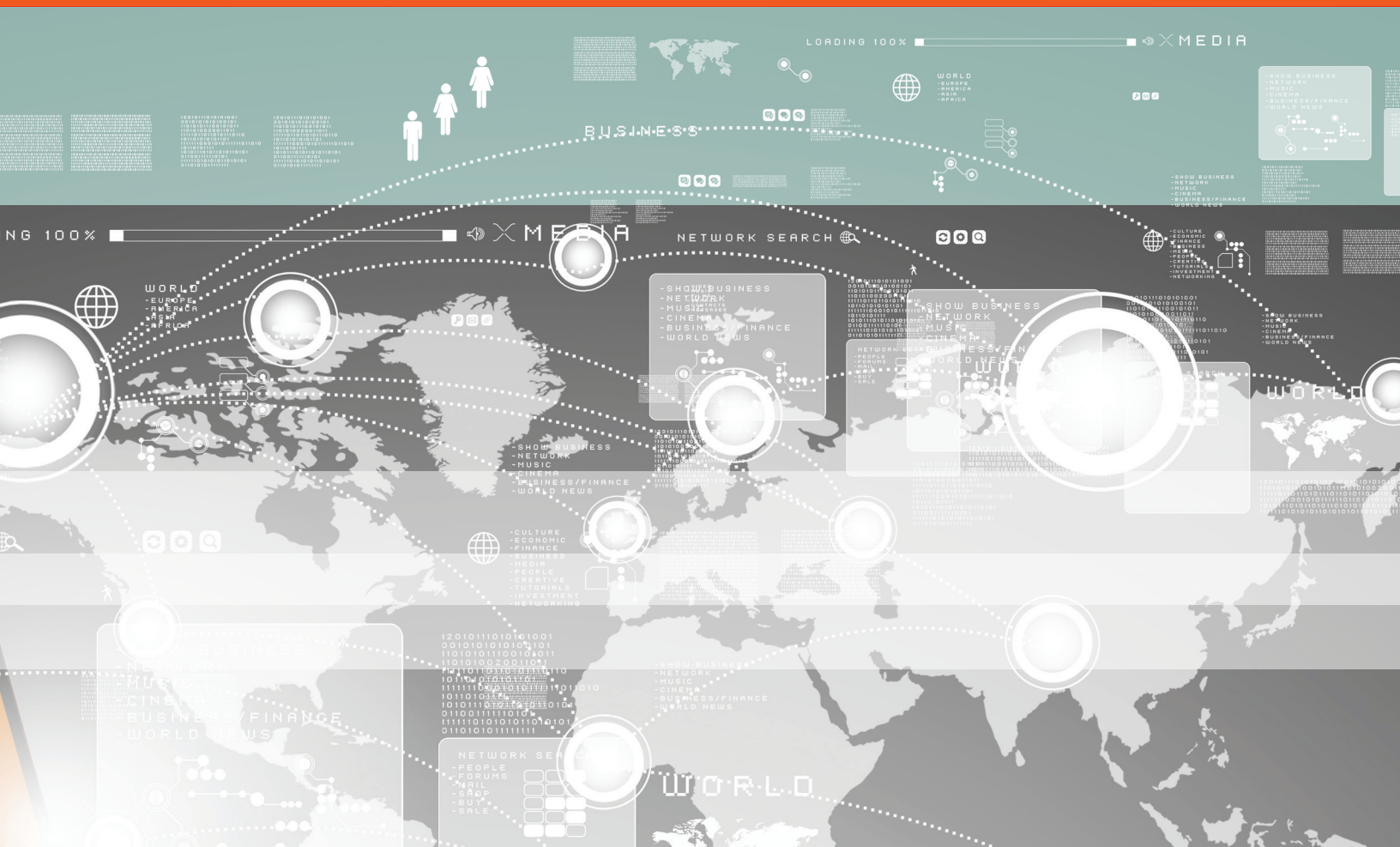
Intelligent Authentication and Fraud Prevention Intelliview

Solutions for Emerging Security Threats and CX Challenges »

opusresearch



opusresearch | Report »

Intelligent Authentication and Fraud Prevention Intelliview

Solutions for Emerging Security Threats and CX Challenges »

In this third 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 beyond voice biometrics to include additional biometric factors (facial, fingerprint, behavioral), fraud detection, digital orchestration, and continuous authentication. This report evaluates 20 firms, both platform providers and core technology providers, to understand their completeness of offerings and ability to orchestrate capabilities into broader solutions that respond to emerging security threats and CX challenges.

»

August 2020

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

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

www.opusresearch.net

Table of Contents

TABLE OF TABLES

Authentication Is Every Company's First Impression

"You never have a second chance to make a first impression" is the advertising slogan of a men's suit maker in the 1960s. It has new meaning and relevance today as a growing number of commercial conversations take place over span of time, using a variety of devices. After Web searches, consultations with trusted "friends" on social networks and navigating through e-commerce websites, the last thing that an individual prospect or customer wants to do rummage through their memory for a password or figure out the answers to "challenge questions."

For decades, bands of imposters have treated contact centers as the weakest links in enterprise efforts to prevent the hacks that lead to loss of customer data or wholesale theft of goods, services and money. Long ago, authentication procedures have replaced "How may I help you?" as the routine first step (more accurately, a barrier) to customer care or assistance. Procedures have been time-consuming, annoying and ineffective. The most popular practices include SMS-based delivery of "one-time-passwords" (OTP) and knowledge-based authentication (KBA). The former is vulnerable to rudimentary "man-in-the-middle" attacks and the latter largely relies on information that imposters can compile from publicly available sources.

Opus Research defines the term "Intelligent Authentication" (IAuth) to capture a range of solutions and offerings that have evolved since voice-based authentication to include additional biometric factors (facial, fingerprint, behavioral), fraud detection, digital orchestration, and continuous authentication.

Accelerating Along the Path to Maturity

From their inception, customer authentication initiatives were concerned solely with using a short list of factors to keep bad guys out while letting validated customers carry out their desired activities. PINs and passwords (something you know) prevailed, augmented by annoying challenge questions or other forms of knowledge-based authentication (KBAs). Too often, they called for customers, themselves, to do the heavy lifting of remembering a password, answering a set of challenge questions or requesting and inputting a "one-time password" as it is displayed on a mobile phone or company-provided "dongle."

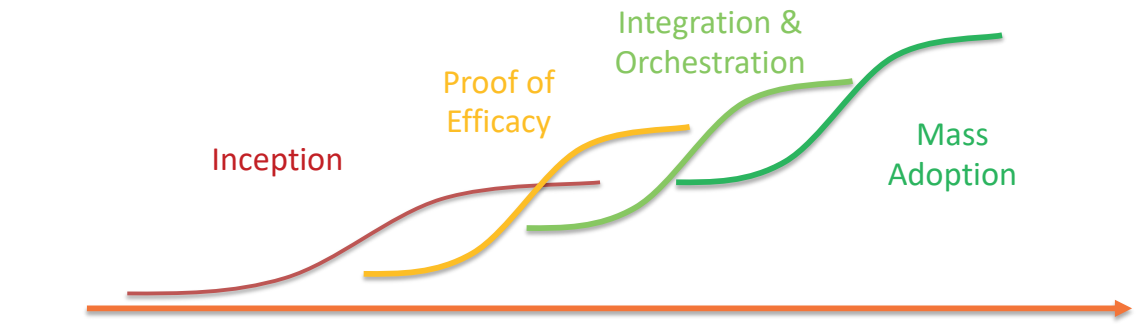
Today's solutions have to do a lot more. Remember: No customer calls or goes online to authenticate; they have a purpose or intent in mind and authentication is a necessary evil. They should be context-aware, meaning that they are able to take a customer's location, past activity, transaction history and current intent into account in order to derive the level of risk to assign to a particular customer or activity. They should involve zero-effort or minimum effort on the part of a customer as they seek to establish a trusted communications link with a brand. The firms that support passive enrollment that can take place in the course of a conversation with a speech-enabled IVR, virtual assistant or live agent earn higher ratings in our evaluation.

Eras of IAuth

IAuth solutions (both platforms and core technologies) evolved in parallel with (and in support of) digital transformation, intelligent assistants and conversational AI. It started slowly at the turn of the century, battling

concern over accuracy and cost-effectiveness. [See Figure 1 below to view the evolution of Intelligent Authentication.] Adoption and implementation accelerated significantly as end user acceptance was clearly demonstrated by early adopters in the mid-teens, and continued to accelerate as the return on investment was proven.

Figure 1:The Eras of Intelligent Authentication Continuum



Factors	Single Factor (E.g.Voice)	2FA	Multi-Factor	Continuity
Barriers to Adoption	Accuracy	End User Acceptance	ROI	None
Context	Automated IVR	Contact Centers	Natural Language Applications	Move to the Cloud
Products and Services	Text-dependent voice auth	Active and Passive enrolment and auth	Multi-layered, risk-aware auth and fraud detection	Continuous, zero-effort auth and passive fraud detection

- **Inception** (2000-2010): The "My Voice is My Password" approach acknowledged that callers were consciously using their voice (something they are) instead of a PIN or password (something you know). Solutions were rigid (text-dependent) and suspect, especially among security professionals who sought "zero false accepts."

- **Proof-of-Efficacy** (2011-2017): Solution providers successfully enrolled a billion voiceprints into systems for banks, telecom companies, healthcare providers and government agencies to speed authentication and discourage fraudulent access. Real-time fraudster detection, employing multiple technologies, including Deep Neural Networking (DNN) in addition to passive voice biometrics, played a big role in justifying the investment.

- **Integration/Orchestration** (2018-2020): UX, Security, and IT architecture professionals join contact center operations staff to integrate a variety of biometrics, risk engines, UX design and other workflow management platforms into real-world solutions. All recognize the value of strong, real-time authentication to improve security, customer experience and personalization initiatives.

- **Mass Adoption** (aspirational): The solution made available by the firms included in this document broadened appeal by fulfilling real-world demand for strong, seamless authentication employing go-to-market strategies that make it affordable for all businesses who have an enduring relationship with their customers. In the post pandemic world, that means there's opportunity in e-commerce, tele-health and e-government, in addition to banking, finance and telecommunications.

Customer Perspective

"Project started April 2016, with the goal to support security, shorten the handling time and to reduce inconvenient security questions asked for authentication ... Main challenges were legal issues, because of the law for data protection and the question whether to do an opt-in or opt-out ... After a few adjustments the business case could be delivered."

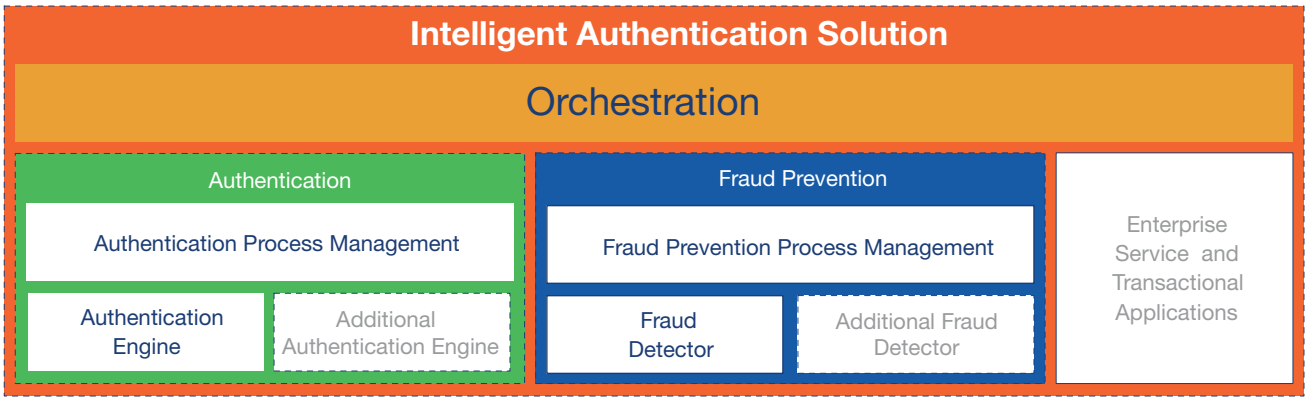
—Global bank with 2.5M retail customers, 300K business customers, 500 call center agents

Focus on IAuth and Fraud Detection

A complete IAuth solution integrates authentication and fraud detection capabilities with the underlying channel technology, the business processes required to enable authentication (such as enrolment and verification) or fraud detection (such as watchlist and case management) and each other to enable secure customer service. In many enterprises this "stack" will consist of a mix of customized or packaged solutions from multiple vendors as well as internally developed capabilities. In Figure 2 (below), we break out the layers and conceptual components of this stack to help readers articulate their requirements more clearly.

As the market for Intelligent Authentication has matured over the last few years, we have seen the development of distinct areas of focus for vendors and interest to enterprises. Vendors can choose to specialize in one or two "core technologies" to support needs or requirements of application developers with integrate solutions. Another category of vendors takes a holistic view more aligned to our definition of IAuth and suited to addressing or orchestrating a full spectrum of authentication and fraud detection functions.

Figure 2: Defining the Intelligent Authentication Stack



SOURCE: Opus Research (2020)

Authentication Stack

The authentication stack, depicted in green above, consists of 2 core components of interest to enterprise users.

- Authentication Process Management - This layer provides the business user-facing features required to enable one or more core engines to be used in an authentication process such as managing user consent, enrolment and verification. In many cases, authentication components only expose an API that can be used by the end-user organisation or systems integrator to develop this component.

- Biometric or other Authentication Engine – The authentication component performs the pattern matching between contemporaneous input and stored templates. In the context of enterprise customer service, it is often a behavioural or physical biometric but can also include knowledge-based authentication processes. In addition to pattern matching must protect itself from understood vulnerabilities, such as spoofing or presentation attack detection.

Fraud Prevention Stack

Similarly, the Fraud Prevention stack similarly consists of 2 layers of interest:

- Fraud Prevention Process Management - This layer is where alarms from one or more detectors are used to evaluate the fraud risk of interactions and trigger the required business actions either in the form of case management or by communicating with other applications.

- Fraud Detector - This is the component that interprets the signal received from the channel into meaningful results such as detecting anomalies in audio or signalling characteristics or matching known bad actors' signatures.

Orchestration

The term "Orchestration" most often refers to the use of automation, algorithms or rules configure, manage, and coordinate computer systems, applications, and services. More specifically it can refer to resources that automate a process or workflow that involves many steps across a multiplicity of systems. In the context of IAuth, orchestration co-ordinates the authentication and fraud prevention processes using additional context from other enterprise transactional or service applications to determine whether interactions or transactions should be allowed to continue with or without additional authentication or fraud prevention steps. This is usually based on some for or "risk score" which in many cases to govern how a company should treat an individual or the specific task that he or she is carrying out.

Orchestration capabilities are often a source of differentiation for providers of full-blown IAuth platforms. A relatively small group solution providers have offerings that sit above Authentication, Fraud Prevention and Orchestration. Through connectors or APIs, they incorporate insights from databases associated with other applications or services that can govern assessment of perceived risk and, the actions that should be taken based on those assessments.

Customer Perspective

"Greatest challenge is to produce a scalable and secure system which can be deployed and consumed easily by businesses and consumers. ... [The solution] replaces all authentication with a voice and face biometric check which is managed by the system prior to being connected to an agent, thus saving agent call time as well as greatly increasing security."

—Commercial Director at UK-based Information Security firm

Two Categories of Respondents

"Do I want a platform from a single vendor or best-of-breed technologies?" is an evergreen question that haunts Contact Center, CX and Security personnel, project managers and procurement professionals regardless of vertical industry or company size.

Customer Perspective

[For selecting a vendor, we wanted] a voice biometrics solution that would be contained within the same suite of applications as voice recording system and workforce management tool ... [It was important to have] ease of access from our users into a single system.

—Banking & Financial Services firm based in Asia-Pacific

To prepare this document, Opus Research conducted evaluation of the IAuth products and services of 20 vendors – 7 "Platform Providers" and 13 suppliers of "Core Technology" that support Intelligent Authentication (IAuth) and fraud detection. These are part of the broad opportunity areas depicted in Figure 2:

- **Platform Providers**: Offer turnkey solutions that support enrolment of voiceprints or other biometrics, active or passive authentication and fraud detection. They augment their offerings with flavors of analytics, machine learning and Deep Neural Networking (DNN) that power risk engines and fraud detection resources. A crucial differentiator is "Orchestration" which employs decisioning engines to inform other elements in the platform based on assessment of real-time input, such as the risk that a particular individual is who he or she claims to be, in a location one would expect them to be, using a device that is associated with them and that there are no other anomalies.

- **Core Technology Providers**: Category describes firms that have hired staff and made continuous investment in technologies that address the challenge of continuous, strong, friction-free authentication to support conversational commerce.

Figure 3: Firms Included in the Inelliview

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.

Company	Category	Distinction
Aculab	Core Tech	API-enabled auth & security
Auraya Systems	Core Tech	Voice Biometrics specialist
Biocatch	One To Watch	Behavior biometrics, AI models
Daon	Platform	IdentityX platform orchestrates multi-factor auth
ID R&D	Core Tech	Cutting edge Voice Biometrics + face recognition, liveness detection
Interactions	One To Watch	Voice Authentication integrated into Intelligent Virtual Agent Platform
Journey	One To Watch	Orchestrating "Zero-knowledge" auth, mutual auth
LumenVox	Core Tech	ASR, TTS, Voice Biometrics, and Speech Analytics
NICE	Platform	RT Authentication, RT Fraud Prevention, AI Continuous Fraudsters Exposure
Nuance	Platform	Largest Voice Biometrics footprint; Applying AI to fraud & orchestration
Nuestar-Trustid	Core Tech	Call center + digital
Omilia	Platform	Conversational self-service
Phonexia	Core Tech	VB, Speech Analytics
Pindrop	Platform	Risk-based auth; fraud detection; incorporating DNN
Sestek	Core Tech	Broad speech tech; active auth focus
Spitch	Core Tech	Core VB, Virtual Agent
Verbio	Core Tech	Voice Biometrics and Speech Processing
Verint	Platform	Voice and Behavioral Biometrics for Authentication and Fraud
VBG	Core Tech	Voice Biometrics specialist, SaaS model; APIs
VoiceIT	Core Tech	Ease of VB deployment and API differentiators

Evaluation Criteria for IAuth

To support purpose-driven conversations between brands and their customers, enterprises need to greet callers, visitors or interactions differently. To do so, they can now apply predictive analytics, deep neural networking and biometric-based authentication (fingerprints, voice, face, behavioral) to establish their identities and get down to business. The goal of these combination of technologies is Intelligent Authentication and Fraud Prevention.

In this document, Opus Research and SymNex Consulting evaluates the companies under investigation with the following attributes in mind:

- Real-time
- Risk-aware
- Adaptive
- Multifactor – including behavioral biometrics
- Multi-layered

All of the firms under investigation are distinguished by the quality of their service offerings. However, they should not be subjected to identical evaluation criteria in order to assist readers in vendor selection.

Simply stated, Platform providers are rated highly for the completeness of their offering and their ability to orchestrate the performance of a variety of capabilities that span friction-free authentication. Core Technology providers, on the other hand, receive high ratings to reflect their investment in unique, distinguished technologies, along with connectors, APIs and a go-to-market approach that is flexible and makes it easy to be incorporated into broader solutions that respond to emerging security threats and CX challenges.

Ones to Watch: New Intelligent Authentication-Aware Solutions

Not category members, but category changers

We take special note of three firms that are included in this evaluation even though their product and services offerings do not map directly to the “Platform” or “Core Technology” categories. Opus Research considers them bellwethers or leading-edge providers of technologies that advance the concept of IAuth, even though there is no basis for head-to-head comparison with other firms in their respective categories. They have built formidable sets of services that combine the principles of IAuth and a subset of components of the overall solution stack.

Journey.ai

Journey.ai offers a “Trusted Identity Platform” to address specific gaps in the digital infrastructure that supports conversational commerce, balancing security, privacy and customer experience across multiple channels. Its “zero trust” approach enables companies to use their mobile apps and smartphones to enroll both customers and agents and, then employs its resources to invoke a variety of authentication factors, including biometrics flexibly. It applies novel techniques for what it calls “mutual authentication” and includes behavioral biometrics as part of the mix of authentication factors in order to support continuous, friction free experience.

BioCatch

Biocatch provides core behavioral biometric technology that builds profiles based on such actions as mouse movements, typing cadence, swipe patterns or device orientation that, when compared to population level profiling can detect fraudsters or imposters. Banks, insurance companies and credit card issuers are finding it to be an important tool for preventing "new account" fraud and detecting imposters, bots and use of "synthetic" people to gain access to existing accounts.

Interactions LLC

Interactions is included because it offers proven voice biometrics-based authentication and fraud-detection capabilities as a natural complement to the broader Interactions' voice virtual assistant. It is not marketed as a stand-alone, core technology; nor is it integrated into a broader IAuth Platform – with hooks into risk and decisioning engines. Opus Research believes that the enterprises that employ Interactions' Intelligent Virtual Assistants will find its resources for enrollment and authentication an alternative worth evaluating.

Intelliview Maps for Platform and Core Technology Providers

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 and 6 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** – Platform providers receive the highest assessments of "completeness" when services and features cover all columns of the solutions stack: Authentication, Fraud Prevention, Orchestration and Applications. Core Technology providers are judged by their relationships ability to integrate with complete solution providers through connectors and applications program interfaces (APIs).

- **Strategic Potential** – For both Platform and Core Technology providers this metric captures how vision and roadmap appeals to current and evolving technology requirements in contact center and beyond. Ability to support multiple factors, such as behavioral biometrics, and incorporate new technologies like Deep Neural Networking are a plus. In addition, the ability to support applications in IoT, intelligent endpoints and mobile. Also taken into consideration are each company's ecosystem of go-to-market partners, integrators and developers.

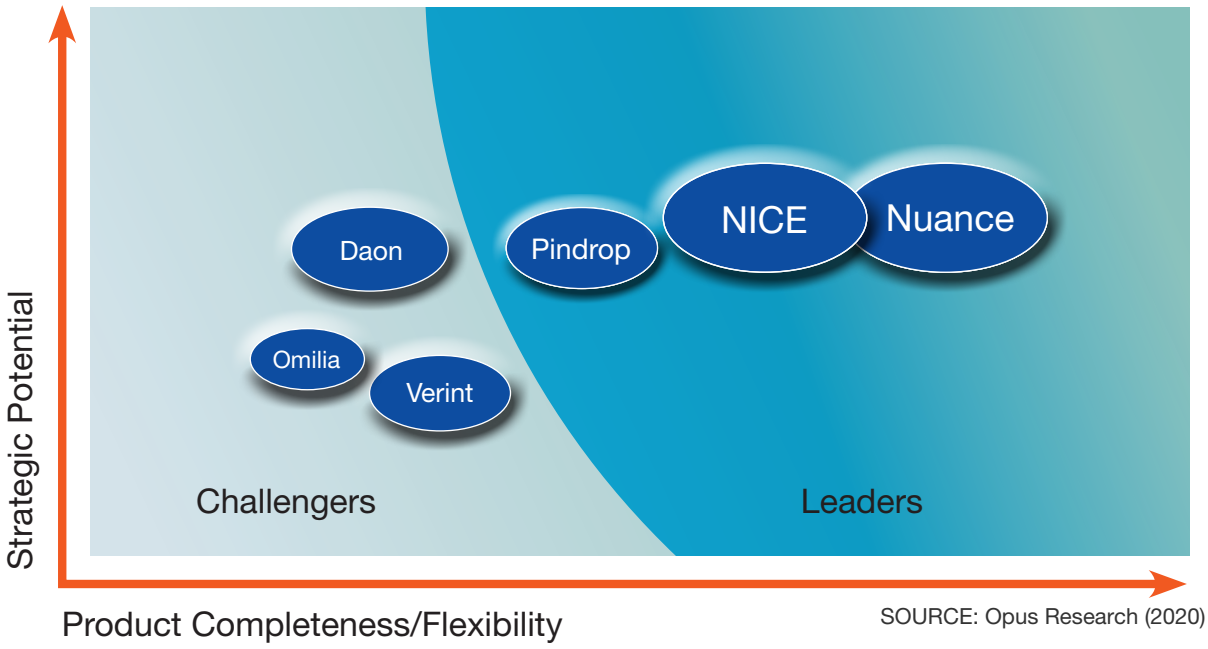
The size of the ovals represent each vendor presence based on company-provided or publicly available information of current financial strength (revenue, profitability, financial banking, longevity and size of customer base).

The colors of the ovals relate to vendor category:

Platform Providers

Core Technology Providers

Figure 4: 2020 Platform Provider Intelliview Map



SOURCE: Opus Research (2020)

- Among the leaders in Platform providers, Nuance and NICE stand out due to their comprehensive authentication technologies, integrated fraud prevention offerings, and strong, established customer bases. Solutions include Nuance's Lightning Engine, ConversationPrint and DevicePrint, and NICE's real-time ENLIGHTEN Fraud Prevention, which leverages AI-infused speech analytics and behavior models to provide real-time feedback to agents.

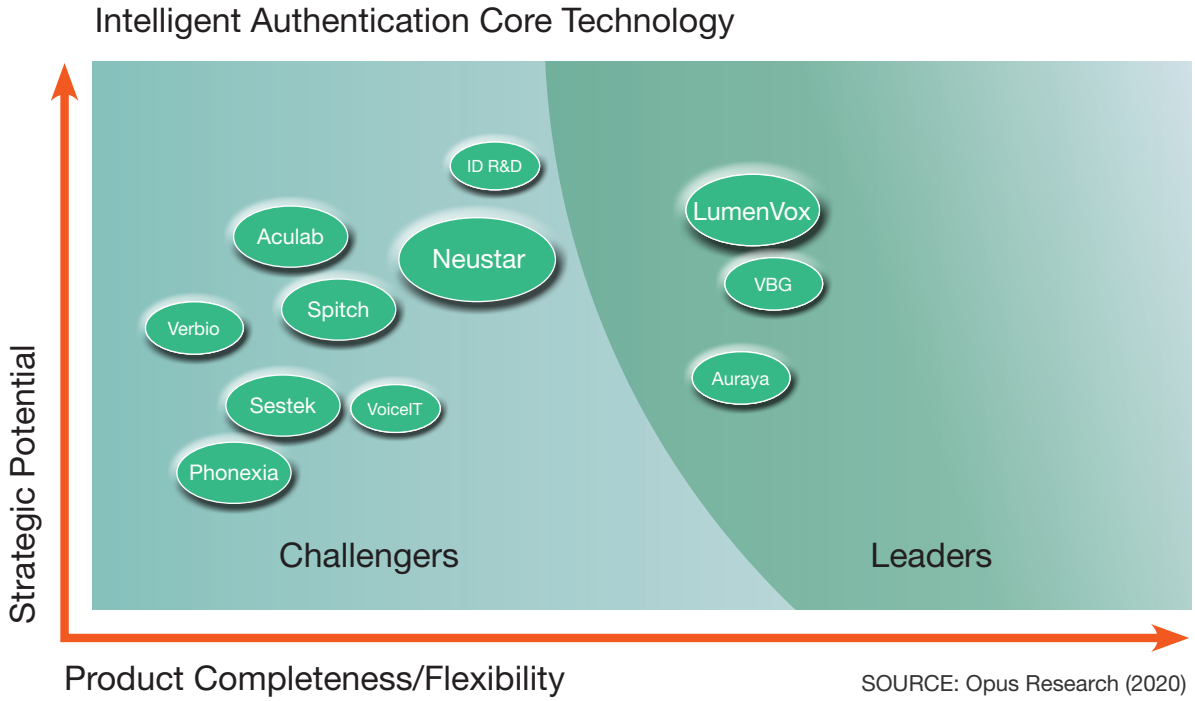
- Pindrop has distinguished itself with its patented technology for risk, fraud and identity verification, leveraging risk-based authentication with access to a large, comprehensive fraudster database.

- Daon has global-scale production deployments, authenticating millions of identity transactions in multiple biometric authentications.

- Verint has long-established expertise in customer engagement and speech analytics, building an emerging roster of authentication and fraud prevention customers.

- Omilia leverages close integration between its authentication engine and conversational AI platform to provide a compelling solution to enterprises looking for both. Its authentication engine is also available as a standalone component.

Figure 5: 2020 Core Technology Provider Intelliview Map



SOURCE: Opus Research (2020)

- LumenVox's merger with VoiceTrust combines a capable Biometric solution provider with LumenVox's established speech recognition, partner relationships and deep integration experience. Voice Biometrics Group (VBG) and Auraya are singularly focused on Voice Biometrics and with millions of enrolled users their solutions benefit from this maturity and deep focus.

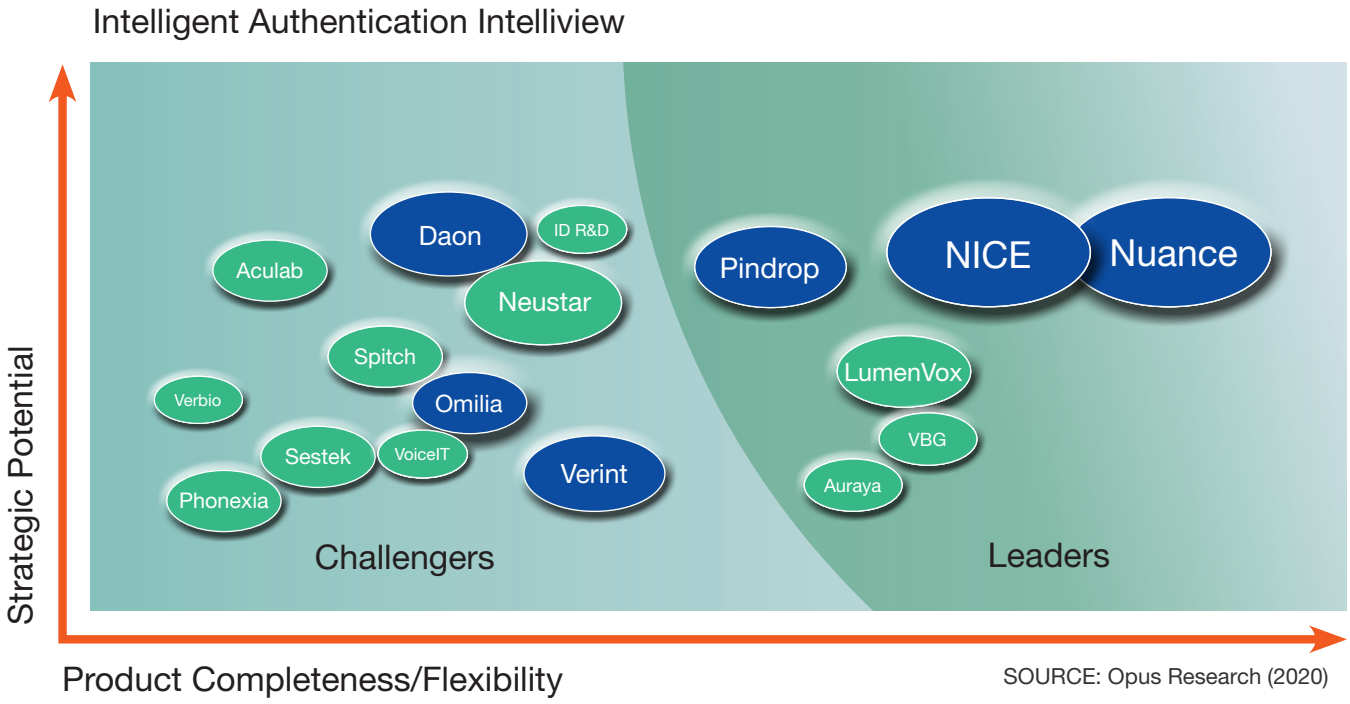
- ID R&D has focused on mobile and application use cases with impressive results from academic and industry tests. Neustar, with the acquisition of TRUSTID, combines cross channels products for digital and call center authentication and fraud use cases.

- VoiceIt's unique as a service proposition requires only a credit card to get started and provides sufficient sample code for the major platforms that develops can get started and deploy applications in hours not months.

- Verbio and Spitch have developed voice biometrics capabilities alongside their wider speech technology portfolio, have several deployments between them and are real challengers in their chosen markets. Aculab brings more than 40 years of experience in signal processing and telephony technologies to challenge the established players in the Voice Biometrics market.

- Turkey-based Sestek includes voice authentication with a broad set of conversational solutions. Phonexia is bringing its market leading government experience to the commercial market.

Figure 6: 2020 Combined IAuth Solution Provider Intelliview Map



SOURCE: Opus Research (2020)

Appendix A – Vendor Profiles

Aculab

Headquarters: United Kingdom
Revenue: $7.5 million
Number of employees: 10

Scope of IAuth Services

Core Products: VoiSentry – Speaker Verification; Speaker Identification; Free VoiSentry developer trial sandbox, integration via flexible APIs

Knowledge Factors: Text-prompted verification scenarios, use of per-speaker pass-phrases

Possession Factors: Dependent on each customer's application; tie the authentication to a specific hardware device or static IP address, if available.

Biometric Factors: Voice only biometric factor available in VoiSentry

Behavioral Factors: Provides language-independent pass-phrase/pronunciation validation to improve security

Additional Channel Factors: Audio quality / coding / channel validation**;** Presentation Attack Detection

Fraud Detection: Covert speaker identification; presentation attack classification (impersonation/mimicry, replay attacks, voice conversion/speech synthesis)

Orchestration: VoiSentry's sensitivity to impostors can be controlled (through the API) on a per-speaker basis; allows a voiceprint to be updated to give improved security.

Implementation

- Offers cloud-based service
- Size of IAuth professional services team: 6
- Pricing: Licensed
- IAuth intellectual property (number of patents/R&D employees?) 4

Future Plans & Vision

- Standards bodies will work together with authentication systems and core technology providers to develop practical and flexible specifications for control and communication between the different components of multi-factor and multi-modal authentication systems.
- Key Differentiators: Integrated multi factor authentication; Language and text independence; Indication of presentation attack type

Auraya Systems

Headquarters: Sydney, Australia
Revenue: N/A
Employees (directly related to IAuth): 15

Scope of IAuth Services

Core Product: ArmorVox™ allows any type of voiceprint (text-dependent, text-independent, digit-independent, text-prompted), spoken in any language; core engine used by Eva to complete omni-channel identity verification, fraud prevention and detection, and voice trait analysis.

Knowledge Factors: First-party knowledge-based questions, PIN/password used in text-prompted mode; embedded in identity validation services used to collect a voice sample as part of a multifactor identity verification process.

Possession Factors: Collect a voice sample as part of a multifactor identity verification process, remote document validation tied to a transaction code for a specific transaction.

Biometric Factors: Voice; passive, active, text-dependent, text-prompted, digit-independent, text-independent, vocal trait analysis and fused speech recognition.

Behavioral Factors: Used with third party identity validation services; voice trait analysis can determine that the gender and age of the voice matches Usage identification/anomaly detection to detect if the correct voice provides the correct response using the authorized device within an authorized time frame; also detect brute force attempts for real or synthetic voice attempts

Channel Factors: Configured to raise security thresholds and require random challenge responses if a user attempts to access an account on an unregistered device Presentation attack detection uses a number of processes to detect different threat vectors.

Fraud Detection: Supports any number of lists, using any type of voice print or vocal characteristics; can be used with shared information or watchlists. Combines text dependent, digit independent, and text dependent prints created from known fraudster recordings; dual look up process to reduce false flags and improve fraudster identification. The biometric data is combined with device ID and any other relevant data to inform decision making in fraud detection.

Orchestration Risk profiling is provided by the application rules engine and can be informed by organization risk engines such as Threat Metrics. Agent web browser provides the information about the user and allows the agent to change the user's biometric status. In addition to the web browser agent interface, EVA can be configured to connect with any other selected agent interface such as Service Now, ZenDesk, Salesforce, to provide identity verification indicators and controls to the agent. Analyst/Investigations Case Management EVA utilizes Amazon Firehose to stream and transform EVA data into a dedicated S3 bucket. From there, it can be consumed by reporting databases and business intelligence services such as Amazon QuickSight providing organizations with the ability to integrate EVA reporting into their chosen reporting engines for contact center, fraud detection and enterprise reporting.

Implementation

- Supports specialist reseller partners as part of solution deliverables such as Digital Channel Transformation, contact center solutions, fraud and risk specialists.
- Primary partners: Accenture (NYC /Global), AI secure biometrics (San Diego/ USA) Amazon Web Services (Seattle/Global), Connect Managed Service (UK), Deloitte (Sydney/ Global), ECS (Scotland/ Singapore), Fujitsu (London/Global), GBG group (UK and Australia), Help Systems (Core Security Boston/ USA), Inference (USA and Australia), PriceWaterhouseCoopers (PWC Auckland), Probe Group (Aust and NZ), Telstra (Aust), Unisys (Virginia VA/ Global), Vodafone (Germany/Global), voice Foundry (Global)
- Deployed in the client's secure cloud or their own on-premise infrastructure or solutions can be a hybrid on-prem/cloud
- Size of professional services team: 8
- Pricing: Per user per annum which entitles every enrolled user to unlimited verifications; Per transaction charges a fee for every enrollment or verification session; Perpetual license scaled by the number of users who can be enrolled.
- IAuth intellectual property Six families, 24 patents total

Future Plans & Vision

Mission of empowering people and organizations to interact and engage with convenience and security in all channels and languages. Enables organizations to reduce complexity, reduce inefficiency, comply with regulations, stop repetitive boring manual processes, protect themselves from fraud and bad actors and gain even more insight and value from their data so they can innovate and serve their consumers better. Key Differentiators include vision for innovation security performance with the most user convenience of any voice biometric technology; Deployment using the clients preferred partner or building in-house resource

BioCatch

Headquarters: Tel Aviv, Israel
Year business started: 2011 (IAuth: 2015)
Investment/Funding: last round, series C, April 2020, $145M
Revenue: N/A
Number of employees: 160

Scope of IAuth Services

New Account Fraud	BioCatch protects new account applications by analyzing a user's physical and cognitive digital behavior to distinguish between genuine users and criminals in order to detect fraud and identity theft and to improve customer experience.
Account Takeover	The BioCatch Behavioral Platform leverages machine learning algorithms to analyze physical and cognitive digital behavior of users across digital channels.
Synthetic ID Fraud	Detection of synthetic ID fraud is very similar to new account opening fraud detection, as cybercriminal will display high familiarity with the process and application from, and low familiarity with the data, whether is it stolen or fake.
Money Mule Identification	Detected via account opening detection methods as well as a range of velocity assessments for account activities, suspected payees and others

BioCatch protects with the following features:

Data validation:	Verifying that data provided in an application is accurate and matches other data sets about the user
Bot detection:	Identifying automated access attempts, either at login or during an application
Device fingerprinting:	BioCatch performs device fingerprinting using web and mobile SDKs. Device elements collected for web include: IP, IP geolocation, time zone, browser type, user agent string, browser cookie, display settings, permissions, as well as a global unique Identifier use is the BioCatch consortium
Remote access detection:	Identifying suspicious access attempts, even through legitimate customer device.
Behavioral Biometrics	Behavioral biometrics analyzes a user's physical and cognitive digital behavior to distinguish between genuine users and criminals in order to detect fraud and identity theft and to improve customer experience. 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
Mobile Emulator Detection	An Emulator is a software application for a personal computer which creates a virtual machine version of a mobile device
Social Engineering Voice Scam	One of the hardest types of fraud attacks to detect. By leveraging advanced data science and AI techniques, BioCatch's solution analyzes more than 2,000 behavioral parameters and generates powerful insights to detect fraud.
Cognitive Analysis	User profiling on the population level. BioCatch analyzes cognitive decisions and choices made by users such as how they input data.
Behavioral Insights	Combines user and population level profiling to determine user intent and emotional state in context of the activity to detect complex situations indicating high levels of risk.
Behavioral Analytics	Analyzing the context of the user activity - amount, payee, last access, previous scoring, sequence of activities and pages visited.
Mobile device theft	Using deep learning models and combining behavioral data and all of the above methods BioCatch is able to detect effectively this type of threat.

Channel Factors: BioCatch performs device fingerprinting using web and mobile SDKs. Device elements collected for web include: IP, IP geolocation, time zone, 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, Wi-Fi, time

zone and global unique identifier. Device profiles are incorporated into the various models to detect different types of financial crime. BioCatch also looks at network elements as well as proxy intelligence as part of the analysis.

Fraud Detection: Customers can use watchlists as part of the policy decision. Elements that can be added to these watchlist are IPs and others. BioCatch has a consortium of global device identifiers that is used for device intelligence across customers.

Orchestration: 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). Customers send risk calls to BioCatch via REST API to receive a risk score and top risk and genuine risk indicators. The API call also contains additional data that is used for risk assessment such as the activity context (activity type, payee, amount, etc.). In addition, the API calls may include external scores to be aggregated by the BioCatch rule engine to create an aggregated risk score or to be used by the policy manage to determine the appropriate action. API responses include the score and top risk and genuine risk indicators, so customers can determine the action to be taken (allow, deny authentication, review, etc.) 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.

Implementation

- Delivery Model: Mostly direct but there are some channel partner engagements as well.
- Primary partners: Experian, Microsoft, ForgeRock
- Service Management: BioCatch is deployed in in Microsoft Azure data centers globally to support its global customer base.
- Size of professional services team: 30
- Pricing Models: For New Account Protection, price is per new account application; for Account Takeover Protection, per user per month; additional percentage of applications/ users, respectively
- IAuth intellectual property: Patent portfolio with 51 patents granted and 20 additional patents filed

Future Plans & Vision

BioCatch will continue to enhance it fraud prevention solution by partnering with customer to identify new threat vectors and new ways to identify user behavior patterns that identify legitimate and criminal activity. Key Differentiators:

- **Breath of data and knowledge incorporated into AI models** - With 10 years of data and experience analyzing digital behaviors, BioCatch has over 70 patents (49 granted, 23 pending) that enable unique methods of collecting, analyzing and profiling more than 2000 critical components of behavior in every one of our 1 billion AI-driven behavior based sessions per month.
- **Continuous visibility and actionable insights** - Providing full visibility into the user activity throughout account lifecycle, from login to logout, to detect the most subtle changes and identify all types of attacks.
- **Why Behavioral Biometrics** - BioCatch Platform profiles the user's interaction with the device looking at over 2000 points of input, creating a unique identifier that cannot be stolen, copied, or spoofed, unlike device and location, ensuring robust, future proof protection.

Daon

Headquarters: Fairfax, VA
Year business started: 2000 (IAuth: 2015)
Investment/Funding: N/A
Revenue: N/A
Number of employees: 150

Scope of IAuth Services:
Enrollment support and account initiation: IdentityX Onboarding provides mobile SDKs, Javascript libraries and REST APIs for capturing a user's ID document, selfie and face liveness. Daon's IdentityX® delivers identity establishment and verification, Multi Factor Authentication, and recovery across all four corners of the customer experience (mobile, web, contact center and physical location).

- **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.
- **Extensive policy control** over all aspects of authentication: modality(s), match thresholds, attempts, device capabilities.
  This provides our 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.** Our core technology has scaled to populations of hundreds of millions. USAA has reported no-problem at a peak load of 750,000 authentications in a day with IdentityX.
- **High-Availability.** Can be deployed in highly-available and disaster recovery configurations.
- **FIDO.** 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.
- **Omni-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's 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 Factors: Daon's 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 include 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.

Implementation

Both direct and channel delivery model
Primary partners: Visa, Experian, Oracle, ForgeRock, DXC, CA Technologies, Deloitte, Avtex, Pragma, Airata, CU*Answers, Gemadec, Mitek, the UPS Store, DTIS
Service Mgmt.: Daon provides managed service hosting in shared tenant environment or via private cloud.
Size of professional services team: 50
Pricing Models: Annual subscription, vary by volume of users
IAuth intellectual property: 160+ patents

Future Plans & Vision

Daon's vision is to create the next generation of omnichannel identity, called "Identity Continuity." It's a vision that encompasses continuity from channel to channel (user experiences are consistent and data flows seamlessly between events, interfaces and workflows), from component to component (security intelligence sharing enhances the speed and performance of otherwise disconnected identity and security tools), and from past to present (past data on users, transactions, and processes make present-day experiences frictionless and more secure).

Key Differentiators:

- Customer trust & ability to execute (successful global-scale production deployments)
    - Chosen to secure more than 1 Billion identities on 6 continents; handles more than 100 Million identity transactions of consequence each day; 250+ major financial firms using our technology
- Broadest and deepest biometric expertise in the world
    - Experienced team of biometric research scientists, product engineers, programmers, and UX specialists; Brought more biometric apps to market than anyone else; Road-tested 100+ third party biometric algorithms in our in-house labs
- Innovative platform offers first and only true omnichannel/cross-channel experience for complete identity life cycle
    - Platform's uniquely flexible, open, and versatile design accommodates a limitless array of channels, use cases, and devices to meet current and future security, convenience, and compliance needs

ID R&D

Headquarters: New York, NY
Year business started: 2016
Investment/Funding: $6M, series A
Revenue: Undisclosed
Number of employees: 40

Scope of IAuth Services:

Enrollment support and account initiation - IDVoice supports cross-channel enrollment. Enrollment can be passive (ask the customer if they would like to use ongoing interaction to enroll once the needed amount of voice has been captured) or directed whereby a user would either speak a passphrase three times or provide 15-20 seconds of free speech.

Authentication: ID R&D has a technology advantage, offering high accuracy on short utterances for Text Dependent, Text Independent and streaming Text Independent. ID R&D offers a multi-modal approach to mobile device biometrics, with the key elements are voice, voice liveness, face (through a third party), passive face liveness, and behavioral keystroke biometrics. Now testing a new generation of "end-to-end" neural networks called d-vectors. This methodology not only increases the accuracy by 30% when compared with x-vectors, but also runs on small NPUs without speech feature extraction support. Also support streaming for continuous verification of the user's voice. The current version of the product utilizes an advanced modified x-vector approach for superior accuracy. ID R&D finished the 2019 NIST Speaker Recognition Evaluation Challenge with exceptionally strong results. ID R&D finished with the best results overall among 50 participants; however, these results are not made publicly available.

Fraud Prevention: Whereas biometrics secure identities, liveness detection products secure biometrics by detecting and stopping spoofing attacks. Products offer accurate, frictionless detection of presentation attacks including recorded voice, synthetic voice, photos, masks, and video. The biggest fraud risk today due to the adoption of face recognition globally is spoofing face recognition systems. To combat this problem, ID R&D developed IDLive Face, a passive anti-spoofing solution that achieved ISO 30107-3 compliance for Level 1. Recently announced IDFraud Contact Center, a product which uses Text Independent Voice Biometrics and speaker diarization to identify repeat fraud in the telephony channel. ID R&D also develops products specific to particular use-cases, for instance our clusterization anti-fraud capability aimed to identify individuals opening multiple accounts (within the same call center) under multiple assumed identities.

Orchestration: ID R&D provides an app framework called SafeChat to help implement the multi-modal biometrics in a conversational interface.

Biometric Factors

- *Voice:* Voice liveness and commitment to R&D in these areas is demonstrated by results in the NIST speaker recognition and ASVspoof challenges. Also provide voice anti-spoofing capabilities that distinguish real voices from recordings and synthetic speech.
- *Face:* Face liveness detection is a primary focus. Passive approach requires no participation by the user. This is different from most products which use an active approach, requiring users to undergo a challenge response activity whereby they must blink, turn their head, correctly position their face within a frame etc. ID R&D is committed to a frictionless liveness detection approach.

Behavioral Factors: IDVoice can check age and gender

Channel Factors: Provide presentation attack detection for voice and face biometric authentication. The technology can be used across channels including physical devices.

Fraud Detection: IDFraud Contact Center matches callers against watchlists of known fraudsters as well as recently opened accounts to determine if the same voice is connected to multiple identities. *Cross matching* and in addition to looking for the same voice across different claimed identities, we support age and gender detection for comparison against available identity information on the user.

Implementation

- Delivery Model: Primary delivery model is channel
- Please list your primary partners: NDAs prohibit us from sharing the names of many of our largest partners. Publicly announced: FacePhi, Innov8tif, TECH5, Zenoo, Hive.id, and RelyComply (BusinessOptics)
- Service Management: All products are available as SDKs or as a docker image for deployment by the client or partner on premise or in their secure cloud environment; IDFraud Contact Center product is cloud-based.
- Size of professional services team: Don't have extensive demand for professional services for; preference to make products simple and easy to deploy
- Pricing: Per user per year, per transaction, per device, or as a perpetual license.
- IAuth intellectual property: Approx. 75% staff is R&D (30 employees); 10 patents pending

Future Plans & Vision

ID R&D is intensely focused on advancing the science of biometrics through performance breakthroughs and innovation. We have extensive expertise in speech and biometric technologies, unique data collection methodologies and capabilities, and the industry's leading R&D team. Efforts have resulted in top rankings in the largest independent benchmarks in the world -- with the #1 ranked voice biometric matching software for accuracy and speed (NIST speaker recognition challenge), the #1 ranked voice anti-spoofing software (ASVspoof). Additionally our passive facial liveness detection product is ISO/IEC 30107-3 compliant.

Unlike other biometric companies, ID R&D places great emphasis on user experience. Believe that all Enterprise-Scale Intelligent Authentication should evolve to become continuous, frictionless authentication where security is stronger than today with zero effort from the user. This belief drives product development strategy and results in products that are unique in the market, such as SafeChat™ and IDLive™ Face.

Within each biometric technology area, ID R&D offers features that are important differentiators:

- Cross-channel support for voice so the same voice biometrics template works in the call center and mobile and web SDKs for mobile devices as well as servers
- Passive facial liveness with no need to blink, turn a head, smile, or move the device, ideal for testing liveness in a KYC onboarding process and when authenticating using a selfie (face image).
- High performance on ultra-short utterances (both text dependent and text independent)

Interactions

Headquarters: Franklin, MA
Year business started: 2004 (IAuth: 2016)
Revenue: ~$100M (2019)
Number of employees: N/A

Scope of IAuth Services

Knowledge Factors: First-party knowledge-based questions; third-party identity validation services; password/PIN

Possession Factors: ANI, IMEI

Biometric Factors: Voice

Behavioral Factors: N/A

Channel Factors: Device identification/anomaly detection (EMEI); Network identification/anomaly detection (Third party partnership)

Fraud Detection: Watchlists based on one or more factors; Voiceprint blacklisting; ANI blacklisting

Orchestration: Authentication decisioning making (i.e. confidence in claimed identity)

Implementation
Direct delivery model; Cloud based, fully hosted and managed
Pricing: Services + annual license fee or enrollment Fee + transaction price per authentication; success-based pricing
IAuth intellectual property: 16 patents

Future Plans & Vision
Voice interface is the next generation of user experience. As IoT becomes mainstream, more and more everyday devices and appliances will get connected to the Internet and voice will be the primary mode of interface. Voice biometrics will become an essential feature to protect users.

Due to the increased incidents of security breaches and identity thefts using knowledge-based authentication, consumers need more secure methods such as voice biometrics and/or multifactor from vendors when dealing with personally identifiable information (PII, PHI, PCI). Voice biometrics works on all telephonic devices and doesn't require additional technology on users end, making it the ubiquitous authenticator for voice-based authentication.

Key Differentiators:
Natural Complement to Voice Virtual Assistant

Simple integration – Collect User Consent to Enroll
- No IT involvement/equipment purchase for client
- Can replace arduous Authentication procedures
- Rapid deployment with IVA

Passive & Active Enrollment & Authentication
- Built with Unified Interactions Curo Speech and Language Platform
- Our adaptive technology makes the voiceprints stronger with every call, to combat temporary voice changes, aging etc.

Competitive Pricing
- Implementing Voice Biometrics does not need to cost millions – the Intelligent Virtual Assistant product provides conversational customer service, with voice biometric authentication as an add-on service in the hosted IVA.

Journey

Headquarters: 1999 Broadway #1470, Denver, CO 80202
Year business started: 2016 (IAuth: 2020
Investment/Funding: $2.5M
Revenue: N/A
Number of employees: 34

Score of IAuth Services:

Enrollment support and account initiation: Journey makes it possible for businesses to use their existing mobile apps to enroll end-users, whether they are customers or representatives of the business, in highly regulated environments. Including but not limited to a new banking customer opening a KYC compliant account in ~1 minute with greater security than is achieved in a physical branch or a patient enrolling in a telehealth application complete with verifying their ID and health insurance.

Authentication: Journey turns the business's existing mobile application into the biometrically powered source of truth that ensures their customers are who they say they are, and they can leverage that app-based proof in voice, chat/digital, and physical interactions. Journey additionally makes it possible to flexibly invoke a variety of biometric factors, from device based (i.e. FaceID) to cloud-based, which combine to reach up to 1:billion accuracy in <2 seconds. Journey's primary method of delivering transformation to user experience, security, and digital privacy in the contact center is through simplifying the world through the end-user's mobile app.

Fraud Prevention: Journey's approach is to make verified digital identity the root of trust and in the process creates a powerful new tool to prevent nearly all forms of online fraud. One unique aspect is ability to apply technology to voice calls into and out of the contact center. Journey is leveraging zero knowledge cryptography to keep private data private. Credit and debit card payment information is processed using zero-knowledge protocols and the only the success/fail results presented to contact center agents.

Orchestration: Journey's Orchestration Engine (JOE) and technology is built to solve for the trusted identity needs at the core of user experience, security, and digital privacy across the whole customer lifecycle – from enrollment, to authentication, to interactions and transactions. Patent-pending Zero Knowledge Identity Network leverages zero knowledge cryptography, proxy re-encryption, homomorphic encryption (among other techniques) to orchestrate the transmission of data from source to requester and pre-ordained regulators without having access to, or the keys to gain access to the data.

Knowledge Factors: Journey's platform makes a verified identity the root of trust for all online transactions and as such, it takes a big step in making KBA and other forms of security questions obsolete. Introducing scalable MF biometric authentication allows for accuracy, eliminating any need for static or dynamic KBA.

Possession Factors: Businesses mobile applications that are equipped with Journey's technology become capable of validating the legitimacy of a wide array of physical documents from around the world, matching the user to their document, and automatically collecting the important data needed to check internal and external databases such as a BSA compliant KYC check or a check of other industry or company specific licensure and documentation.
Remote document validation: In addition to the previous answer regarding physical document validation, Journey empowers business with the ability to facilitate electronic document signing while on a call. Agents can remotely deliver documents to callers via their app or a browser and request signatures. If performed through the app, Journey links the biometric authentication to the digital certificate of the signature.

Biometric Factors: Journey is a strong believer in face biometrics as the technique that can yield the greatest available combination of user experience and accuracy. As such, Journey makes it possible not only for businesses' mobile apps to communicate to their back-end infrastructure and agent environment when a user passes a device-based facial recognition such as FaceID, but to also flexibly deploy our secondary facial matching and liveness check which utilizes a fully independent biometric template saved in the cloud.

Behavioral Factors: Provided via ecosystem of technology partners.
Channel Factors: Provided via ecosystem of technology partners.
Fraud Detection: Provided via ecosystem of technology partners.

Risk profiling: Anomalies can be detected both through Journey's core feature sets such as around behavioral biometrics, as well as through a business's traditional infrastructure, and Journey provides unique and critical abilities for the business to act on those anomalies to resolve situations before they translate to fraud by bringing in step-up authentication and 3rd party validation such as dynamic KYC checks.

Agent User Interface: Journey's contact center integration integrates seamlessly with any agent environment. Specific features can be integrated as standalone widgets, and/or the full environment can be modified to deliver Journey's Zero Knowledge Queries (status of verifications ranging from identity to payments, rather than source data)

Implementation

Delivery Model: Primarily a channel model utilizing contact center partners.
Primary partners: Cisco, Avaya, Acqueon, aceyus, CBA, CCT, Customer Dynamics, Eventus, New Era, Onestream, Princeton
Service Management: Journey's Trusted Identity Platform is a Cloud-based SaaS offering. It is also available in a private cloud configuration.
Size of professional services team: 15
Pricing: Success-based identity transactions, SaaS offering.
IAuth intellectual property: 13 patents (pending), 25 employees dedicated to R&D

Future Plans & Vision

Journey's Trusted Identity platform solves a major problem for contact center voice channel caller identity verification and authentication by offering a competitive replacement for KBA that offers orders of magnitude in improvement of identity veracity And it is equally effective across all digital channels.

Key Differentiators:

- Journey is a Zero-Knowledge Service Provider: Entire orchestration of Trusted Digital Relationships is accomplished without need to see any identity data that traverses the network
- Journey brings the full identity verification and authentication capabilities from the mobile app world to the Contact Center voice channel.
- The Enterprise has a New Tool -- Trusted Digital Identity: Table is set to identify the human being on the other end of a voice call. Journey is tool to prevent fraud, eliminate friction from the customer experience, attach identity to Card Not Present transactions and solve the network security problem.

LumenVox

Headquarters: San Diego, CA
Year business started: 2001, merged with VoiceTrust in 2018
Investment/Funding: Privately funded and profitable.
Revenue: N/A
Number of employees: ~40

Scope of IAuth Services:

Enrollment support and account initiation: Available Capabilities. Authentication and fraud prevention are the main priorities for LumenVox Security. Without successfully onboarding a client's users, that goal cannot be achieved. To that extent, we provide best practice enrollment and account initiation recommendations across modalities using active, passive and fraudster watchlist biometrics data.

Authentication: Primary Focus / Experience. LumenVox has developed a state-of-the-art proprietary voice biometrics engine for passive and active voice biometric authentication inclusive of native multifactor and multi-tenancy support, with regular version updates. LumenVox voice biometric authentication provides for rapid delivery with a prebuilt agent interface that does not require lengthy API integration and may be delivered via cloud, premise, or hybrid models.

Fraud Prevention: Primary Focus / Experience. LumenVox Passive Voice Biometric Authentication analyzes voiceprint data to build watchlists through voiceprint mismatches. Every incoming call can be evaluated against known fraudster voiceprints in real-time, alerting contact center agents of suspected fraudster activity. LumenVox Fraud Scanner conducts near real-time fraud detection, enabling batch comparisons of caller audio to known fraudster watchlists after call completion. Advanced fraud detection capabilities are already robust including clustering, ANI velocity checks, playback detection, and synthetic voice detection. As the fraudsters evolve, so too will LumenVox Security.

Channels Supported

- IVR: Primary Focus / Experience: LumenVox active voice biometrics increases IVR containment while simultaneously improving security.
- Contact Center: Primary Focus / Experience: LumenVox Passive Voice Biometrics authenticates users during natural conversation with a live agent, reducing agent handle time. It also detects fraudsters both in real time and offline, as needed by the customer.
- Mobile: Primary Focus / Experience: Mobile applications may integrate LumenVox active voice biometrics as step up authentication, part of a multifactor solution, or as a point solution, such as automated password reset.
- Web: Available. Because voice quality varies from device to device, LumenVox continues to monitor how voice over web will be used. In theory, voice via web can be authenticated using voice biometrics. In reality, very few applications will leverage the technology that way because of microphone quality on devices.
- Chatbots and automated intelligent assistants: Available through 3rd party partner integration.
- Messaging platforms: Emerging
- Intelligent endpoints (smart speakers, IoT sensors, etc.): Emerging
- Other

Knowledge Factors: Primary Focus / Experience. LumenVox' security solutions leverage knowledge-based authentication as method of authentication in addition to voice biometric authentication. Knowledge-based authentication is often used for establishing ground truth.

Possession Factors: One-time passcode generation: Primary Focus / Experience. Some solutions benefit from step-up two factor authentication that includes an OTP to the user's mobile phone for high risk transactions. The LumenVox solution can send a request to a third-party outbound SMS aggregator and/or mobile push application to achieve this extra layer of security when needed.

Fraud Detection: Existing capability. LumenVox Security Suite provides a fraudster voiceprint watchlist, ANI watchlists and ANI approved lists.

Orchestration: Authentication decisioning making - LumenVox provides alerts that can be consumed by third party fraud detection and authentication decision making platforms that leverage voice biometrics as well as outside factors. Risk profiling - LumenVox Security can flag high risk callers and send those alerts in to fraud management solutions, stopping transactions before the fraud is executed. Agent User Interface - LumenVox provides an agent user interface for both authentication as well as fraudster detection however most customers choose to integrate the LumenVox results into their own agent desktops and fraud case management solutions. Analyst/Investigations Case Management- LumenVox Security Suite can provide input to fraud case management systems.

Implementation

- Delivery Model: Over 90% of LumenVox' sales happen through the channel.
- Primary partners: Primary LumenVox partners are Genesys, Avaya, Cisco, plus the associated implementation partners. Since LumenVox is a partner-centric company, LumenVox also sells through and/or partners with the following: Aspect, Twilio, Blueworx, IBM, Speech-Soft/Konnektive, Swampfox, ConvergeOne, Enghouse, Enacomm, Interactive Northwest, M&C Associates, Televoice, Vox Networks, OneVault, EarthBend, Cognizant, Cerium, Capgemini, Avtex and numerous others.
- Service Management: LumenVox is currently deploying private cloud solutions based on market demand. Based on shifts in buying patterns, public cloud deployments are expected in late 2020.
- Size of professional services team: 9
- Pricing: Current pricing models include both perpetual and term licensing based on call volume; flexible pricing plans including risk/reward models that allow LumenVox to share in the successes of the customer. This flexible licensing is how LumenVox provides superior quality technology for lower total cost of ownership (TCO) for customers and partners. Implementation pricing is consistent; however, additional licensing discounts are considered based on volume. Factors that LumenVox considers include: integration requirements, requests for customization, the use of ASR/TTS, length of contract, payment terms and bundling of multiple solutions.
- IAuth intellectual property: Over 15 patents and 10 R&D employees

Future Plans & Vision

LumenVox sees biometrics as a key part of securing omnichannel customer experiences, which is why the LumenVox Security Platform supports not only our cutting-edge biometric engines, but also natively supports multi-factor decisioning using a unique Workflow Management-based approach. To provide our customers with the greatest convenience and functionality, a single deployment of the LumenVox Platform can support voice and facial authentication, fraud detection, and MFA in various configurations for multiple tenants. Integrating with the LumenVox Authentication Platform solution is flexible – either through SIP, VoiceXML/CCXML, our mobile application framework, or directly with our REST APIs.

Key Differentiators

- Universal Voiceprint: capability to utilize one passively created voiceprint for multi-modal use
- Proprietary audio pre-processing algorithms provide more accurate results in challenging environments
- Flexible licensing and pricing structures enable LumenVox customers and partners to rapidly deploy and scale its Fraud and Voice Biometric products for faster time to market and a more competitive total cost of ownership.

Neustar

Headquarters: Sterling, VA U.S.
Year business started: 1998
Year IAuth market contribution started: 1998
Investment/Funding: privately held
Revenue: N/A
Number of employees: 200

Scope of IAuth Services:

- Only Call Center + Digital solution applicable in a majority of use cases in those channels.
- Call center authentication that confirms inbound calls are from unique, physical devices to function as an ownership factor of authentication
- Fraud prevention that provides a Trust Indicator and other data elements to identify calls that may be spoofed, hacked, virtualized or otherwise manipulated

Modalities Supported

- Voice
- Online: mobile web, native browser.
- Call Center

Channels Supported

- Mobile
- IVR
- Contact center
- Web
- Mobile Web

Knowledge Factors

- None

Possession Factors

- Phone-based ownership factor authentication using one time passcode generation
- Phone-based ownership factor authentication for call centers using network forensic call inspection withing the phone network

Biometric Factors

- None

Behavioral Factors

- None

Channel Factors

- Device identification/anomaly detection
- Network identification/anomaly detection

Fraud Detection

- Watchlists based on one or more factors
- Consortium/shared watchlists based on one or more factors
- Cross matching one or more factors across different claimed identities
- Other

Orchestration

- Risk profiling (i.e. anomaly detection)
- Authentication decisioning making (i.e. confidence in claimed identity)

Implementation

- Delivery Model: Both direct and channel
- Primary partners:
  - Digital: Experian, Socure, Threatmetrix, InAuth, Iovation
  - Call Center: NICE, Nuance, Avtex, Coop, Altigen
- Service Management: Certain products offer hosted and private cloud.
- Size of professional services team: ~10 for risk use cases.
- Pricing: Transaction volume
- IAuth intellectual property: Patent #'s – 8,238,532 | 9,001,985 | 9,264,536 | 9,762,728 | 9,871,913

Future Plans & Vision

Vision for Enterprise-Scale Intelligent Authentication & Fraud Prevention

Authentication across Call Center (could be used for Digital Contact Center but still needs to be tested) and Digital channels.

Key Differentiators

- Internally built expertise and cross channels products for digital and call center authentication and fraud use cases.
- Neustar's view is informed from its multi-dimensional view of customers and use cases in the areas of marketing, telecom, fraud prevention, compliance and compliance.
- Call center authentication:
  - Uses unique network forensic technology to inspect calls and calling devices within the phone network to deliver a deterministic authentication token
  - Combines TRUSTID authentication service with Neustar's OneID dataset to deliver a solution that uniquely automates both caller authentication and identification.

NICE

Headquarters: Raanana, Israel
Year business started: 1986; M&A: Nexidia (2016), inContact (2016), Satmetrix (2017), Workflex (2017), Mattersight (2018)
Year IAuth market contribution started: 2016
Revenue (either estimated or publicly available) $1.5B revenue
Number of employees (directly related to IAuth): 80

Scope of IAuth Services:

Enrollment support, account initiation: Passive enrollment with a live agent; historical enrollment; active

Authentication: 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: mobile, IVR, virtual agents, voice, etc.

Fraud Prevention: Proactive Fraudster Exposure capability in the NICE Real-Time Authentication (RTA) solution exposes unknown fraudsters automatically in a daily manner by detecting the abnormal behavior of a specific voice across multiple accounts and calls. Based on unique machine learning technology, the capability allows organizations to automatically prevent fraud before it happens by identifying previously unknown fraudsters and blocking them from committing fraud. Using speech analytics, behavioral analytics , call velocity, phone number verification and more, the identified suspected fraudsters are given a risk score, and then sent for further investigation, added to a watch list of fraudster voiceprints and blocked in the future. Entire process happens automatically, eliminating manual, expensive and time-consuming checks.

Orchestration: RTA provide out of the box multi factor solution using phone number verification and using behavioral analytics. When performing authentication NICE RTA employs a decisioning engine to select the optimal methods for authentication for all types of interactions and transactions between customers and agents. For our customers, that means that our decisioning engine can select the correct authentication methods per customer/interaction to provide the best customer experience for the agent and end-user while maintaining compliance with multi-factor authentication.

Contact Center: Core of NICE's RTA solution. During the first few seconds of a natural conversation between an agent and a consumer, the consumer is being authenticated in the background in a seamless way. The agent then receives a real time notification indicating whether this consumer is valid, and shall proceed to service or whether it is a suspected fraudster. Based on NICE's Contact Center expertise, this authentication can be done on multiple call types (some are stated below) such as Multi beneficiaries, on behalf conversation, etc.

- **Speaker change detection** – RTA provides the ability to automatically invoke authentication request at any time during a call, weather it is in the beginning of the call or during the call. Therefore, authentication can be automatically invoked repeatedly during a call and automatically detect that the speaker on the line has changed and notify the agent about the change.
- **Continuous Authentication** - authentication can be automatically invoked if there is the need for additional authentication, step-up authentication or repeated authentication.
- **Behavioral consideration –** RTA can detect abnormalities in caller's behavior such as the use of synthetic devices or the use of recording to bypass authentication

Mobile: RTA is the only solution that offers passive authentication in every channel thanks to our single voiceprint capability that allow our customers to enroll once and to be authenticated in every channel . This of course include mobile, chatbots , Web and Intelligent endpoints etc. Provides a simple API for bots/Virtual agents with a short audio snippet.

Knowledge Factors - Nice RTA focus on providing a strong authentication methods . As all our customers already have knowledge factors we enable our customers to add our VB solution either an authentication replacement or as part our customer multi factor strategy .

Biometric Factors NICE RTA is built on top of our proprietary engine for voice biometrics. NICE's Fluent engine is built on the strength of our market-leading NICE Nexidia Analytics platform as part of a wider initiative at NICE to infuse analytics into everything that we do. It use machine learning capabilities for creating a voiceprint of a specific person and to perform real time comparison of caller's voice to the voiceprint stored on file . In additional using advanced AI capabilities it blocked known fraudsters and expose unknow fraudsters.

Behavioral Factors NICE's vast portfolio includes market leading solutions for customer behavior and speech analytics. These solutions are leveraged by RTA to gain insights about the action the user is trying to do , user behavior, language being used in a call, sentiment and key words. Using Deep Neural Networks and machine learning, these insights are leveraged to improve the authentication and fraud prevention process, making it easier to provide excellent service to legitimate customers and stop fraudsters before the cause any harm.

Fraud Detection RTA provides the ability to create a blacklist of fraudster voices. This blacklist is used in real time during a call, where the caller's voice is compared to all the voices in the blacklist and if it matches one of them the agent will get a notification and the fraudster will be blocked. Easily updated via a user interface manually or automatically using Proactive Fraudster Exposure capabilities.

- DeepFake Detection – Deep Neural network to detect and expose fraudsters using deep fake technologies in order to mimic user voice.
- Replay Attack Detection -- AI capabilities to detect fraudsters playing a recorded voice in order to bypass the authentication or to perform a fraudulent activity .
- Number Spoofing detection - As part of our Multifactor offering, RTA can detect if the calling number is spoofed and if so, alert the agent and ensure that the user won't be authenticated.
- Virtual device - As part of our multifactor offering, RTA can detect if the caller is using a virtual device that might indicate that there is more risk on the call and in such cases take it understand consideration as part of the authentication result.
- Number recently ported - As part of our multifactor offering, RTA can detect if the number recently ported (e.g.: in the last few hours) as this may suggest that this is a fraudster call.

Implementation

- Delivery Model: Some channel, mainly Direct
- Primary partners: Global - More details are available here.
- Service management: Cloud and hosted as part of the NICE CXone offering
- Size of professional services team: Based on needs as multiple teams support multiple products.
- Pricing: Perpetual license or SaaS depending on the deployment model chosen
- IAuth intellectual property: https://www.nice.com/patents/

Future Plans & Vision

Voice biometrics as the primary method for real-time authentication and fraud prevention in the contact center. Such technology should be delivered as part of a holistic, end-to-end multi-factor authentication and fraud prevention solution addressing the specific needs of the contact center starting with connectivity to the CCI systems, getting and managing end-customer consent, managing vast amounts of voiceprints and connecting to agents' desktop.

Key Differentiators:

- RTA is the only solution that offers a single voiceprint across all channels
- Passive Historical Enrollment ™ - Enables the use of historical recordings for the creating voiceprints.
- Proactive Fraudster Exposure – Built-in application in RTA that automatically scans calls and exposes suspected fraudulent behavior, using voice biometrics, speech analytics and call velocity

Nuance

Headquarters: Burlington, MA, USA
Year business started: 1992
Revenue: ~$1.5B
Number of employees: ~8,500

Scope of IAuth Services:

Enrollment support and account initiation: Supports enrollment across channels. In all deployments, a caller goes through a voice enrollment process either passively speaking with an agent in the case of a call center, or actively using a passphrase. For digital channels, enrollment can be triggered via APIs for voice, behavioral and facial biometrics.

Authentication: Nuance delivers a wide variety of authentication methods including Active (text-dependent) voice biometrics, Passive (text-independent) voice biometrics, call validation, ConversationPrint (choice of vocabulary, grammar and sentence structure), DevicePrint (a unique print used to identify the device based on acoustics and channel), Facial Recognition and Behavioral Biometrics. Nuance's Lightning Engine allows for text independent authentication in the IVR, achieving high accuracy using very short utterances. Intelligent detectors provide familiarity or risk signals to provide confidence to the authentication decision. Nuance also provides the ability to add additional biometric and non-biometric modalities through plug-ins, and a built-in risk engine to manage the authentication and fraudster detection processes across multiple factors.

Fraud Prevention: Nuance provides the ability to detect fraud across voice and digital channels, and a consolidated view of risky activity across all channels. Nuance can detect and analyze all currently known fraud characteristics within channel (voice and digital). These include the identification of the voice characteristics of the fraudulent caller (voice biometrics), enabling the Fraudster's detection, identification, and subsequent prosecution in a court of law based on biometric evidence.

Nuance can detect a fraudster through their speech behavioral characteristics, notably their choice of vocabulary, grammar and sentence structure (ConversationPrint). Nuance provides the only fraud prevention solution to identify a fraudster with two independent biometric factors within the voice channel. In addition to voice and speech characteristics, Nuance can detect and analyze characteristics produced by the device (DeviceID) and the network (ChannelID) used to conduct the phone call. A unique print can be created to identify a fraudster's device (DevicePrint). Beyond detecting audio characteristics in a call, Nuance can also detect fraudulent behavior, such as the use of bots, automated tools and call patterns.

In addition, Nuance detects all known spoofing attacks within the phone channel, including recording attacks (Playback Detection), text-to-speech voice attacks (Synthetic Voice Detection) and phone number attacks (ANI Spoofing Detection). In digital channels, Nuance can help detect new account fraud and account takeover. Based on the patterns of user interaction with the device, Nuance can detect if it's a human or a bot, if it's behavior that appears to be fraudulent, or if it is consistent with the behavior of the legitimate user. Nuance can also detect suspicious activity in the session such as bots, remote access sessions, the use of untrustworthy VPNs or IPs, and other risky characteristics.

Capability Orchestration: Nuance provides the ability to orchestrate the business logic behind the enrollment, authentication and fraud detection flows; the interaction between the solution and the customer's infrastructure; and integrations with 3rd party systems within the customer environment.

Biometric Factors: Voice, Face, Fingerprint (can integrate results from fingerprint sensors, such as Touch ID), Behavioral biometrics.

Behavioral Factors: ConversationPrint is a patent-pending technology that analyzes language patterns for authentication and fraud detection. Additionally, Nuance has a range of behavioral detectors that extend to voice and chat, for example, detecting type, tap, and text.

Channel Factors: Able to determine the device and model used during an interaction as well as changes and anomalies in the way the user is using a device. Determines if the device has changed to indicate a potential fraudulent call or web/mobile session. Analyzes the meta data in an interaction to identify inconsistencies and determine potential spoofing (i.e., a spoofed phone number). Detects geographic location via the phone network and network-based anomalies of all devices such as IP change and remote access sessions.

Fraud Detection (Watchlists): Nuance has a real-time and offline Fraud Detection capabilities that allows for the creation and management of watchlists. A watchlist can contain both biometric, device, and behavioral prints. As such, a watchlist can include voiceprints, ConversationPrints, and DevicePrints, along with additional metadata such as gender, language spoken, and other characteristics can variables that can be leveraged to prioritize alerts. Nuance DataShare consortium is a Nuance-based information sharing portal that allows a participant to share with other organizations certain data of individuals who are known to have committed or have attempted to commit a fraud against one or more organizations (the "DataShare Service").

Orchestration: Nuance can orchestrate the business logic around enrollment and authentication flows and decision making. Confidence in the claimed identity can be based on multiple layers of security, including the biometric factors and additional familiarity and risk signals.

Agent User Interface: agent GUI shows the authentication status and result. The GUI does not require any action on the part of the agent or person interacting with the agent. In the standard, out-of-the-box GUI, results are displayed to the agent in easy to understand color coded responses, such as green for a successful authentication, red for an unsuccessful authentication and purple for the detection of a fraudster. In addition, the GUI can showcase additional metadata on the caller, including their voice classification, the caller's ANI and any other metadata that could be of use to the agent.

Analyst/Investigations Case Management: Fraud will be detected and reported in a couple of ways. First, representatives can be notified when a caller's voice has matched the voiceprint of a known fraudster in the watchlist in real time. This allows the representative to take action immediately. Nuance also has offline capabilities that allow potential fraud to be investigated by fraud analysts and addressed after the fact, such as speaker clustering and backward search.

Implementation

Delivery Model: Both direct & channel
Primary partners: Avaya, Cisco, KCOM, Genesys, Carahsoft, Accenture, Telstra, Diagenix, Vodafone, Deloitte Presidio
Service Management: Provides a hosted cloud service; support for private cloud deployments will be available early 2021.
Size of professional services team: 700 global individuals
Pricing: Tiered pricing, based on volume, per transaction – this allows price to adapt to different sizes and volumes of deployments
IAuth intellectual property: 1450 R&D employees, 3,000+ patents

Future Plans & Vision

Provide timeless seamless, efficient and accurate authentication and fraud prevention through biometric, across devices and interaction channels. Within 5 years, there will be no more knowledge-based authentication. Nuance will deliver a comprehensive Security solution to address all Enterprise authentication and fraud prevention needs, and continue to invest in core research, including the development of novel anti-spoofing technologies to stay ahead of emerging threats.

Key Differentiators:

- Comprehensive integrated authentication and fraud prevention solution across digital and voice channels – delivering end to end customer experience, with both on-device and server-side biometric processing.
- Industry leading authentication success rate and fraud prevention rate, outcome of continuous investment in core technology (including 4th generation DNN). Notably, Lightning Engine allows for text independent authentication in the IVR, achieving high accuracy using very short utterances.
- Customers report better ROIs than organizations that deploy competing solutions, higher fraud loss savings and higher authentication success rates.
- Transparency, making all checks available to the customer to explain the detailed reason why a specific authentication response was returned is much better than the black box approach.

Omilia

Headquarters: Limassol Cyprus
Year business started: 2002
Investment/Funding: $20M (Q1 2020)
Revenue: N/A
Number of employees: 60

Scope of IAuth Services:

Enrollment support and account initiation: The enrollment in Omilia deepVB®, is performed through one of the following methods — or a fused approach: Text-Independent — Voiceprint creation is performed by having DiaManT® continue listening after the call is escalated for this purpose and while the customer is being authenticated by a human agent, ensuring the authenticity of the voice sample. Or Dynamic Text-Dependent — Voiceprints are created by having DiaManT® capture specific words, like the last 4 digits of the SSN, the customer's zip code and other words frequently found in a banking application, such as "balance", "account" etc.

Authentication: Omilia deepVB® verifies customers passively within the IVR or Mobile App, while they engage freely in a natural language conversation with DiaManT®, or while they speak with an agent. User authentication is performed in real-time in the background via scoring the speaker's voice match to the voiceprint, from first dialog step, and during every step until hang-up.

Fraud Prevention: Omilia's fraud detection solution uses the Omilia NLU Application, and leverages Omilia's DiaManT® service to provide detection capabilities for proactive end-to-end fraud prevention real time. The fraud prevention mechanisms are built into the natural language conversational solution, meaning that DiaManT® can change the call flow, challenge the caller with additional security questions, as well as analyze various call/session characteristics.

Knowledge Factors: 1st Party Knowledge Based Questions -- any internal data metrics (account number, email address, etc.); 3rd Party Identity Validation Services (ANI spoofing, CRM history)

Biometric Factors: Voice only

Behavioral Factors: Omilia anti-fraud solution takes various behavioral patterns into account in order to correctly identify fraudsters. In particular, the following are monitored: recalling rates (time intervals and frequency); wording & speech (speech durations, specific words used, number of words, etc.); nature of requests (e.g. account information vs payments). Using these parameters, a "fraudster" profile is built across domains and applications. At the same time our solution detects any outliers or anomalies both on a call and user level against the regular conversational flows.

Channel Factors: The Omilia Anti-Fraud solution can blend capabilities from additional data sources (ANI validation, characteristics in the signaling protocol, and one-time passwords transmitted via SMS) to assist in the detection of fraud across channels. Omilia's Anti-Fraud platform also extends to Enterprise Fraud Systems.

Fraud Detection: Omilia's Anti-fraud solution operates on two types of profiling: application users and authentication assets. A watchlist is maintained for every user and authentication asset, storing a wide range of important information, mainly related to: usage & context, frequency, association with other users/assets
Using this methodology, Omilia's Anti-Fraud solution can cross match different assets across different user identities and vice versa and therefore carry out complicated extrapolations involving a wide list of parameters and factors. Anti-fraud solution also uses a blacklist/whitelist functionality. Confirmed suspects are stored in the blacklist which is used as an extended watchlist feature. On the other hand, the whitelist is used to identify clear users that have suspicious behavior due to the nature of their operations, such as big companies, testing numbers or surveys.

Orchestration: The anti-fraud solution scores a session, user and asset with a fraud score that can be viewed as the solution's confidence level for labelling: the session as potentially fraudulent, the user as a suspect fraudster and the asset as targeted for fraud/breached. This fraud score is built by taking into account the profiles summarized above together with the traits of the current session. This happens by fusing together a rule based approach with a machine learning classifier. The rule-based approach works on pre-aggregated data used to build the profiles for users and

assets, while the ml classifier fits the current session into its robust classification model and returns a confidence score.

Implementation

- Delivery Model: Direct and channel are supported; strong integrations with telephony platforms
- Primary partners: Concentrix, Genesys, and NICE inContact
- Service Management: Omilia offers the Omilia Cloud Platform ("OCP") as a public cloud platform: a range of ready-to-consume Conversational AI services, which provide the core building blocks; willing and able to accommodate private cloud hosting options.
- Size of professional services team: 930
- Pricing: When sold as part of a conversational UI, biometrics is sold in a “per minute” price that adds on to our core Conversational Speech to Text services. When VB is sold “stand alone” (not as part of a Conversational Speech to Text), there are two price points--a “per enrollment” fee, and a “per validation” fee.
- IAuth intellectual property: 3 patents pending, 27 R&D employees

Future Plans & Vision

Key Differentiators

- Strong, seamless integrations to Hosted Contact Center (CCaaS) providers ○ Many deployments on NICE inContact and Genesys
- Built for passive enrollment and verification of speakers ○ Live deployments at financial institutions
- Native integration into Conversational Platform (e.g. IVR or mobile app channels) ○ Part of our core technology stack (not added in via 3rd party)

Phonexia

Headquarters: Brno, Czech Republic, European Union
Year business started: 2006 (IAuth: 2017)
Investment/Funding: Self-funded
Revenue (either estimated or publicly available): $2,4M USD
Number of employees: 55

Scope of IAuth Services:

Enrollment support and account initiation: Primary focus; Phonexia Voice Verify can enroll the caller after 20 seconds of net speech and create a voiceprint.

Authentication: Phonexia Voice Verify can identify a caller after 3 seconds of net speech with over 92% accuracy. The accuracy increases further even after those 3 seconds, and the cases when a speaker changed during the call are detected as well.

Fraud Prevention: Phonexia VoiceVerify can reliably identify fraudsters trying to impersonate legitimate users via the phone. Advanced protection against synthesized or computer-alternated voice is coming soon.

Modalities Supported

- Voice Primary
- Text
- Video
- In-Person

Channels Supported

- IVR Primary (OOB)
- Contact Center Primary (OOB)
- Mobile Secondary (the integration of the technology needed)
- Web Secondary (integration of technology needed)
- Chatbots and automated intelligent assistants Secondary (integration of technology needed)
- Messaging platforms
- Intelligent endpoints (smart speakers, IoT sensors, etc.) Secondary (integration of technology needed)
- Other

Knowledge Factors: Phonexia Voice Verify is based on voice identification and is ideal to enhance or ideally replace knowledge-based authentication (e.g., users no longer need to remember PINs, passwords, security questions, etc.).

Behavioral Factors: Phonexia technologies can identify 68 languages and dialects, as well as a speaker's gender and their age group, all just from speech. Phonexia's speech-to-text technology can also transcribe speech to text in 14 languages and dialects. However, these technologies are not part of Phonexia Voice Verify as an OOB package.

Channel Factors: Presentation attack detection - Anti-spoofing providing protection against PAD is expected in production in H2 2020. It leverages proprietary in-house research & technology (research already done with positive results).

Orchestration: An ongoing decision making in real-time during the whole call to identify the change of a speaker. The confidence threshold is adjustable based on the FAR/FRR trade-off desired by a client, and there is continuous recalculation during the call.

Implementation

- Delivery Model: Primary Direct, Secondary Channel
- Primary partners: Integrators, VADs, VARs, OEM, agents
- Service Management: Support on-premise & private cloud deployments
- Size of professional services team: 5 highly technically skilled pre-sales engineers
- 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: Proprietary voice technologies with IP rights for them. Some of them were researched during collaborative research of the Phonexia research team and the Brno University of Technology's Speech@FIT research team.

Future Plans & Vision

The current focus is on the quality and speed of our primary use cases – the authentication of a caller based on free speech in an on-premise or private cloud environment. The speed and quality of verification is key to our service – our differentiator. Next steps for this year are the protection against emerging modern ways of voice spoofing & seamless scalability in the cloud as preparation for the SaaS model. Next year will enhance our product with 1:N fraud detection (a blacklist shared amongst customers) to increase our use case coverage. The current strategy's vision is to provide Voice Verify completely as a SaaS product.

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

Headquarters: Atlanta, GA
Year business started: 2011 (Fraud: 2012, Auth: 2015)
Investment/Funding: $213M through 5 funding rounds, including $90M Series D funding from Vitruvian Partners Google Ventures and Andreeson Horowitz
Revenue: N/A Private
Number of employees: 220+

Scope of IAuth Services:

Enrollment support and account initiation: Pindrop Passport supports a multifactor enrollment process. Passport encourages an optimal amount of interaction required by the caller for voice, device, and behavior prints to be of use during the authentication process.

Authentication: Pindrop Passport authentication leverages a combination of multiple factors, risk assessment and streamlined authentication policies to perform call center authentication via phone channel. Pindrop has a partnership with Transmit Security that allows us to extend IAuth and Fraud detection capabilities across multiple channels in the contact centers including web, mobile, chat and other. Pindrop Deep Voice for IOT is an authentication solution to verify user identity on smart home devices passively and with ultra-short utterances. Deep Voice is a cloud based as well as embedded SDK solution that is (i) Accurate: based on the latest generation DNN engine, Deep Voice demonstrates a 100% increase in accuracy (lower Equal Error Rate) compared to previous generation solution (ii) Dynamic: Deep Voice is robust to speaker and channel variance across enrollment and authentication (iii) Secure: robust against synthesized voices, and voice distortion.

Fraud Prevention: Protect analyzes thousands of indicators across the fraud event lifecycle - from account mining and reconnaissance in the IVR to social engineering attacks against agents. As agents engage with callers, Protect analyzes audio, voice, and metadata of the caller using (i) Voice biometrics for comparing suspect caller voices to known fraudsters (ii) Behavioral analytics to detect abnormal or suspicious calling patterns and non-monetary prior transactions (iii) Deviceprinting using over 1300 audio artifacts with patented Phoneprinting™ technology (iv) Pindrop Intelligence Network Fraud Consortium checking calls against the world's largest fraud profile database (v) Account Risk calculations (multi-call risk analysis and account activity monitoring to identify compromised accounts and fraud clusters)

Orchestration: Pindrop's joint orchestration platform enables creation of a consistent and comprehensive risk assessment chain across all channels of a call center including the phone channel, chats, online, mobile, IOT, ATM and other access points The joint solution allows Pindrop to (i) manage suspicious call, transaction, and customer account activity by consuming direct API (ii) Receive feedback from cross-channel, high-risk events to enhance its fraud detection models (iii) create additional insights that can be used to flag at-risk customer accounts (iv) send risk feedback to other fraud detection platforms under the Orchestration umbrella for suspicious activity detection.

Biometric Factors: Voice: Pindrop Deep Voice 3.0 is the latest generation Deep Neural Network (DNN) based voice biometric engine that underpins both IAuth and fraud detection solutions. Deep Voice 3 is built on a re-architected neural network and is designed to improve accuracy while recognizing the speaker's voice with less speech. Overall accuracy of Deep Voice 3 improved by 100% over Deep Voice 2 in terms of lowered Equal Error Rate (EER).

Behavioral Factors: Pindrop tracks behavioral factors such as DTMF keypresses, calling patterns, account mining, reconnaissance, robotic dialing and other factors in the IVR as well as at agent leg, that either help compare caller against an established user profile or to identify anomalous / suspicious behavior that could be compared against a fraudster database.

Channel Factors: Pindrop Deviceprinting and Toneprinting capabilities enable identification of device associated with a caller as well as help identify the risk associated with anomalous caller behavior. Pindrop has a native integration with Verizon and partnerships with major carriers to identify network characteristics based on SIP header metadata that can be leveraged for identification as well anomaly detection purposes.

Fraud Detection: Pindrop provides Day One fraud detection using advanced metadata analysis including; ANI blacklist, ANI velocity, ANI Risk, phone number lookup, and gateway numbers. In addition Pindrop can enroll caller profiles including voiceprints, phoneprints and blacklisted ANI that can be used to compare against repeat callers to identify suspicious indicators. Pindrop Fraud Consortium is the shared intelligence from existing Pindrop customers analyzing 1.5 million confirmed fraud phone calls across various verticals. Fraud Consortium includes multiple risk

factors and identifiers associated with known fraudsters that provides pre-ring risk assessment for first time as well as repeat callers for authentication and fraud detection. The Consortium also enables Pindrop customers to prevent known fraudsters and repeat attackers from enrolling as genuine customers. Real-time updates from Pindrop customers identify risky ANIs. The Consortium is constantly evolving to enhance risk intelligence and provides risk foundation for the entire Pindrop Platform. The confirmed fraud database also fuels machine learning engine modeling to optimize fraud intelligence for a specific customer

Orchestration: Pindrop Passport provides authentication score, caller ID validation and risk rating that helps customers operationalize the authentication decision. Customers can leverage the authentication feedback in accordance with authentication policy to remove KBAs or provide step up authentication as necessary. Pindrop Protect provides risk scores and fraud alerts that can be operationalized in the IVR and contact center as well as in online channels. Protect IVR risk assessment (behavior analysis, account mining, reconnaissance, robotic dialing etc.) helps identify anomalous patterns and combines the call risk score with account risk feedback from customers which can be used to place a mark-and-monitor flag on the user account

Implementation

- Delivery Model: Both. 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 and Telnorm
- Service Management: Pindrop provides fully cloud based and on-prem solutions
- Size of professional services team: 30
- Pricing: Enterprise solutions: Tiered by call-volume (higher volumes reduces the price); IoT: by device, transaction or user
- IAuth intellectual property: Patents: 30, R&D employees: 85

Future Plans & Vision

Pindrop® solutions establish the standard for security, identity, and trust for every voice interaction. Pindrop® solutions protect contact centers of the largest banks, insurers, and retailers in the world. Using patented technology that extracts an unrivaled amount of intelligence from every call encountered to score for risk, fraud and identity verification.

Key Differentiators

- Risk Based Authentication: Passport leverages industry leading, proprietary Pindrop risk engines to perform a risk assessment on every call.
- Pindrop Intelligence Network including fraudster database and Consortium: Access to the world's most comprehensive and largest database of known fraudster profiles which goes way beyond a blacklist and includes carrier profiles, behavioral patterns, and reputation risk derived from more than 1.5B calls analyzed.
- Machine learning driven Carrier Signaling Metadata analysis: Through native carrier integrations, Pindrop can perform deep metadata analysis from the SIP header data that cannot be altered by malicious actors.

Sestek

Headquarters: Istanbul, Turkey
Year business started: 2000 (IAuth 2010)
Revenue: N/A
Number of employees: 70

Scope of IAuth Services:

Enrollment support and account initiation: Provide the API which allows variable enrollment scenarios (opt-in, opt-out) among supported channels. Consistency of samples are also analyzed to detect voice changes which is endangering factor to enrollment process.

Authentication: Capable to authenticate users by both active and passive usage scenarios. Voice modality is required for authentication on deployment channel. Authentication results have confidence levels. Clients can implement other authentication factors based on biometric results to mitigate their security risks. Error types (FA, FR) can be adjusted to provide a trade-off between security and customer experience.

Fraud Prevention: Audio files of known fraudsters can be added to Blacklist Identification solution. The system also checks the blacklist members while enrollment and authentication processes. Liveness detection is primary fraud detection feature for synthesized/recorded voice attacks. Brute force detection is also available to prevent brute force attacks on same user or on different users. Users can be suspended automatically by the system if any type of fraud is detected. Listed anti-fraud features work to prevent frauds in real-time.

Orchestration: Orchestration module is responsible from the execution of scenario flows. Utterances and written requests can be handled separately in the same flow to provide an omnichannel experience. Audio files provided by the client application can be sent to an in-house or 3rd party APIs to be processed (Speech Recognition, Authentication, etc.). Channel data (User info, preferences) & attachments can be handled to provide a customized service. Context awareness & the capability of integration with 3rd party APIs allow Orchestration to adapt any business scenario needed.

Behavioral Factors: With the integration of Sestek speech recognition (SR) technology, static or dynamic content can be used in active authentication scenarios.

Channel Factors: Defined whitelisted clients only can be permitted to access on-premise biometrics services.

Fraud Detection: Blacklist Identification based on voiceprints of fraudster audio records. Consortium/shared watchlists applicable if clients collaborate with their archives. Cross matching applicable with partner integrators' applications which has capability to identify other identity factors.

Orchestration: Authentication decisioning making supported by Sestek Orchestrator Service, Hummingbird IVR: Risk profiling supported by Sestek Orchestrator Service

Implementation

- Delivery Model: Both direct and channel
- Primary partners: Eleveo (formerly ZoomInt), Genesys, Avaya, NEC, Cisco
- Service Management: Both managed service, private cloud, hosted)
- Size of professional services team: N/A
- Pricing: Biometrics process user-based (enrollment) and request-based. It varies by the size of implementation.
- IAuth intellectual property: US9462134B2 - Method enabling verification of the user ID by means of an interactive voice response system (12 R&D employees for this project)

Future Plans & Vision

IoT based IAuth solutions will be more practical by increasing voice activity handling capabilities of voice biometrics to gain better authentication results under environmental instability due to external sound effects. Voice Biometrics will also be able to make decisions with the assist of collection and training of users' behavioral data like speech temperaments.

Key Differentiators:

- Flexibility for unique business flows and platforms
- Voice print adaptation
- Single voiceprint for multiple channels

Spitch

Headquarters: Zurich, Switzerland
Year business started: 2014 (IAuth: 2015
Investment/Funding: EUR 2.5m, secured out of EUR5.5m of the investment round
Revenue: CHF2.3m for the year ended 31/03/2020
Number of employees: 42

Scope of IAuth Services

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.

Modalities Supported

- Voice
- Video
- In-Person

Channels Supported

- IVR
- Contact Center
- Mobile
- Web
- Chatbots and automated intelligent assistants
- Messaging platforms

Biometric Factors: Voice, Face (through partners' solution)

Implementation
Delivery Model: Direct and via partners' solutions
Primary partners: Swisscom, Adnovum, Avaloq, BSS
Service Management: All of types of service (both cloud-based and on-premise, or in combination)
Size of professional services team: 6
Pricing: Licenses, SaaS, Pay as you go, revenue-sharing
IAuth intellectual property: no patents

Future Plans & Vision
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. We 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. 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 in voice biometrics using text-independent engine, STT, and providing continuous verification over the course of conversations.
- Phonetics-aware 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.

VBG (Voice Biometrics Group)

Headquarters: Newtown, PA
Year business started: August 2009
Investment/Funding: Privately held
Revenue: Private (> $1MM annually)
Number of employees: 12

Scope of IAuth Services

VBG provides enrollment, verification, continuous verification, identification, fraud detection, and classification (channel and gender) via a SaaS model. Emotion detection will be released in early 2021. Production deployments within IVRs, call centers, chatbots, enterprise applications, web applications, mobile applications, and IoT devices.

The VBG Platform generates a significant amount of statistics/metrics on end users as they interact with the various voice biometric services, including match confidences, scoring behavior, etc. As a SaaS model, VBG does not provide a heavy UI, but rather work with customers to fully leverage API's complete set of functions. Have two web-based interfaces – one for demos/development (VBG Visual Demo Center™, and another for configuring and monitoring production operations (VBG Dashboard™).

Modalities Supported: VBG is focused solely on the development of voice biometric core technology and delivery systems. However, do offer SMS code delivery as part of certain specialized use cases via some of our platform partners (Aspect, Twilio, Telnyx, etc.); this is not a large part of business though.

Knowledge Factors: VBG prefers to rely on partners and clients for establishing ground truth relative to end user identity (before enrolling them

Behavioral Factors: The VBG Platform has been performing gender classification for years, as well as gathering usage statistics regarding scoring patterns, typical usage times, etc. Exploring the addition of language detection features via two platform partners.

Channel Factors: The VBG Platform has channel detection capabilities, as well as the ability to detect common forms of attacks. Will be releasing a more advanced version of our DNN-based presentation attack detection system later this year (Q4 2020).

Fraud Detection: For many years, the VBG Platform has supported an unlimited number of comparative databases (customer and/or fraudster) per customer deployment. This allows ability to construct customized lists based on the specific factors of interest to customers (and flexible as data factors are/are not available). Consortium-based fraud watchlists are possible and currently working with a company who wishes to build a consortium identity model. However, many companies remain resistant to sharing voiceprints – and legislation is increasingly making it more difficult to do so.

Orchestration: Raw scores with confidence (probabilities) have been in the VBG Platform since our earliest days. The latest refinements of DNN models, with different scoring options to provide greater accuracy/confidence over time – both globally across a deployment and on a user-by-user basis. This is of course an area of on-going R&D (and always will be).

The VBG Platform also has scoring/usage profiling to help external rule engines make decisions about anomalies, and we have some simple, built-in rules available as well. Support outbound alerts based on user behavior changes (unusual number of failures, unusual usage, etc.). Most of the more sophisticated partners and clients prefer to consume statistics from our API and leverage their own rule engines.

The VBG Dashboard (web-based UI for deployment configuration and real-time system monitoring) is regularly used by SMB personnel (support/agents) to review specific user behavior (and past statistics/behavior), to assist with troubleshooting, to help evaluate speech samples for potential fraud, etc. More common for customers to perform integrations and light feature development within their preferred agent interfaces – and only include the data/metrics they desire.

Implementation

- **Delivery Model**: Majority of VBG's sales occur through channel partners, though do have many direct customers, sourced primarily through website, trade show networking, and word of mouth.
- **Primary Partners**: publicly named: https://www.voicebiogroup.com/partners.html
- **Service Management:** SaaS model with production deployments in most of the popular public clouds, such as: Alibaba Cloud, Amazon EC2, Microsoft Azure, and IBM Cloud. We also have hard iron U.S. deployments in RackSpace and LiquidWeb. Have numerous private (premise) deployments globally. The VBG Platform is Java-based, parallel-processing enabled, and runs equally well under Windows or Linux server environments (Linux is preferred however).
- **Size of professional services team**: 3 people regularly involved with PS functions, due to business model, on-boarding process, and importantly – the type of partners and clients targeted
- **Pricing:** "Pay by usage" scenarios, a monthly subscription model featuring numerous tiers; "pay by user" scenarios, a licensing model that offers unlimited transactions for a specified number of users, where one user = one unique voiceprint. VBG will also develop custom or hybrid pricing for special circumstances or unique opportunities.
- **IAuth intellectual property:** VBG has no patents, nor current plans to pursue them; have numerous novel/proprietary techniques that could be pursued for patenting.

Future Plans & Vision

VBG's overall mission has changed little since inception: to provide accurate, high-quality voice biometric services via a flexible and scalable SaaS model, and in a far more accessible and cost-effective manner compared to competitors. The combination of accessibility and value remains a critical component of future vision for authentication and fraud prevention. On the deep research side, team is preparing a new set of synthetic speech detection tools – which will be available in production later this year. These tools will complement existing tools for brute force attack detection, spoof detection, etc.

Key Differentiators:

- VBG is U.S./Private: VBG can make the right decisions if and as needed – not subject to outside advisors who are naturally impatient, or who may not understand the intricacies of the VB marketplace as we do.

- Flexibility / Integration Ease: Not limited to "Windows only" and in fact can be Linux or Windows or both. Further, can be deployed anywhere (VM or hard iron) and deploy in HA configurations natively.

- Simple, Scalable, Real-Time Voice Biometrics: More recent efforts to develop plug-ins to several common call center technology platform providers is perhaps unique to a company this size. Combined with the streaming media receiver component of the VBG Platform, can take fully load-balanced RTP and Web Socket traffic from numerous platforms, all by filling in a few form fields.

Verbio

Headquarters: Barcelona
Revenue: N/A
Employees: N/A

Scope of IAuth Services

Knowledge Factors: First-party knowledge-based questions; Biometric voice fingerprint
Possession Factors: Voice validation, One time passcode generation
Behavioral Factors: Content identification/anomaly detection via voice
Additional Channel Factors: Spoofing attack detection, Presentation attack detection

Implementation

Delivery Model: Direct & channel
Private cloud
Size of professional services team: 12 people
Pricing: Corporate licenses, perpetual licenses, monthly rental subscription model, pay-per-use model (based on transactions)

Verint

- Headquarters: Melville, NY 11747 USA
- Year business started: 1994 – M&A Verint Identity Authentication & Fraud Monitoring: Victrio (2013), Contact Solutions (2016), NextIT (2017), Voice Vault (2018)
- Investment/Funding: Verint-wide invested 18% of total/global FY2020 revenue into R&D
- Revenue: $1.3B (FY 2020, ended Jan 31), $847M was Customer Engagement Solutions (including fraud & biometrics)
- Number of employees: 6400 (global)

Scope of IAuth Services

Enrollment support and account initiation: Verint supports an enrollment process where customers create voiceprints via assisted and self-service channels, either actively or passively.

Authentication: Verint supports authentication via any channel where the customer uses his/her/their voice (e.g., phone, IVR, IVA). The solution can passively authenticate the voice independently or actively authenticate through a text-dependent statement (e.g., "My voice is my password").

Fraud Prevention: Once a voiceprint is created, Verint's Fraud Detection solution conducts an analysis to see if the voiceprint matches those of potential fraudsters on a fraud blacklist. Verint also performs dual screening during a call, comparing the voice to an existing fraud database in addition to authentication. Additionally, the Verint's solutions provide upstream detection before fraud occurs; detect actionable intelligence from behavior, interaction and telephony analytics; detect changes in fraud patterns, creating unique, real-time threat assessments for each caller; and provide "Account under Attack" notifications to other enterprise fraud protection solutions.

Orchestration: Verint offers customers the ability to embed authentication and fraud detection into processes and workflows. 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. APIs enable departments to incorporate authentication and fraud detection seamlessly into existing processes and workflows driven by third-party applications. Additionally, APIs can pull watchlists created by the self-service channel's voice biometrics and behavioral analytics solutions and use them to detect potential fraudsters in other channels. The solution can generate a one-time password to a customer's cellphone to verify identity during the interaction.

Behavioral Factors: Verint can surface conversational anomalies via its Speech Analytics solution and automatically alert fraud investigators to potential new lines of inquiry.

Channel Factors: Device and network characteristics of incoming calls can be used to create a risk score associated with potential bad actors and set fraud-prevention alerts. Verint's biometrics solutions support the ability to detect and block fake audio attacks that leverage audio spliced together from various sources or computer-generated speech.

Additional Orchestration: Verint's solutions can trigger color-coded alerts to notify agents of the customer's status after dual screening: verified identity, potential fraudster/bad actor, unknown voice. Verint's Adaptive Fraud solution analyzes caller behavior and telephony data in real-time to detect fraud patterns and behavioral anomalies and creates a unique threat assessment for each caller. The solution adapts and responds to changing fraudster tactics. Threat assessments can be by caller or account and communicated across enterprise channels to stop fraud at all points of attack. Verint's customizable platform and open APIs enable organizations to build or embed authentication and fraud workflows into the agent desktop, CRM or other investigative tools. Verint's fraud portal provides real-time statistics related to all ANIs on alert and watch listed accounts. Analysts can access activity and create a case, placing a phone number or account on a blacklist or set it to a monitoring state while they conduct additional research.

Implementation

Delivery Model: Both direct and primary
Primary Partners: Verint partner network.
Service Management: Offer both private cloud and hosted.
Size of professional services team: Extensive professional services and Verint technical support

Pricing: Offer both transaction- and licensed-based pricing. Pricing varies by package, size, implementation model and other factors.
IAuth intellectual property: Approx. 30 approved and pending patents around IAFD

Future Plans & Vision

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:

- Over 25 years of experience in the capture of real-time data in the call center, Verint is uniquely positioned to provide a cost-effective biometric solution as an integral part of its recording platform.
- 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, MN
Year business started: 2005 (IAuth: 2007)
Investment/Funding: Angel
Revenue: Private
Number of employees (directly related to IAuth): 7

Scope of IAuth Services:

Capabilities
VoiceIt provides a (Patented) cloud-based, pay as you go, face and voice biometrics platform that empowers you to rapidly build and deploy security solutions. VoiceIt offers multiple modals of biometric security solutions: Voice, Face, and Video (Face + Voice) Biometrics.

Voice Biometrics is an integrated multi-engine identification and verification solution. Providing a Second-Factor of Authentication security in a simple-to-use format with minimal friction. With SDKs available for Android, iOS, and Web Browsers, users are able to access Voice Biometrics without the need for specialized hardware.

Video (Face + Voice) Biometrics is an integrated multimodal and multi-engine identification and verification solution. Providing advanced Multi-Factor Authentication (MFA) security in a simple-to-use format with minimal friction. With SDKs available for Android, iOS, and Web Browsers, users are able to access Video (Face + Voice) Biometrics without the need for specialized hardware.

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.

Enrollment support and account initiation: VoiceIt provided the first zero barrier of entry of biometric platforms via SaaS/Cloud Platform back in 2007. We provide support ticketing systems and account engagement with everyone signing up for a free tier developer account.

Authentication: (voice/callers, live chat, bots/virtual agents) : VoiceIt provides many different types of integration levels when it comes to Authentication. We provide IVR, Mobile (iOS and Android), and Web integrations.

Fraud Prevention: VoiceIt helps companies prevent fraud by helping mitigate fraud access to user account information via our biometric services whether built on the edge or used behind their firewalls with our Wrappers, SDK and On-Premise solutions.

Orchestration: We have a new strategic partner **Autnhive* that will be providing Orchestration services with VoiceIt's biometric services baked inside of Autnhive's offerings.

Modalities Supported
- Voice : IVR, Mobile, and Web
- Face : Mobile and Web
- Video : Mobile and Web

Channels Supported
- IVR : All through HTTPS Post calls.
- Contact Center : Amazon, Twilio, UpWire, and others
- Mobile : iOS and Android
- Web : All Web Browsers that support WebRTC
- Chatbots and automated intelligent assistants
- Messaging platforms
- Intelligent endpoints (smart speakers, IoT sensors, etc.) : IoT devices via Autnhive Platform
- Other : Building Security Access

Behavioral Factors: Developing a new Face Tracking Service with Liveness Challenge Order (LCO) and anti-spoofing and anti-replay attack IP. The future version will learn behavioral aspects of the video sent per user.

Orchestration: Autnhive has baked VoiceIt's biometric services into their Authentication systems; Agent User Interface: Stop Light Thresholds for Agentsa

Implementation

Delivery Model: Direct and Channel via Strategic Partnerships
Primary partners: Autnhive, Twilio, Upwire
Service Management: Cloud-based services available: managed, private cloud, and hosted
Size of professional services team: > 4
Pricing: Pricing is done on a Per API Call method or Per User License depending on implementation
IAuth intellectual property: 1 patent

Future Plans & Vision

Enhance our Speaker Validation (Alpha) to release, and integrate with our strategic partners.

- Key Differentiators:
  - Multi-Engine and multimodal biometric solutions
  - Key Strategic Partnerships like Autnhive

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 diversified advisory and analysis firm providing critical insight on software and services that support multimodal customer care and improved customer experiences. Opus Research is focused on "Conversational Commerce," the merging of intelligent assistant technologies, conversational intelligence, intelligent authentication, enterprise collaboration and digital commerce. www.opusresearch.net

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