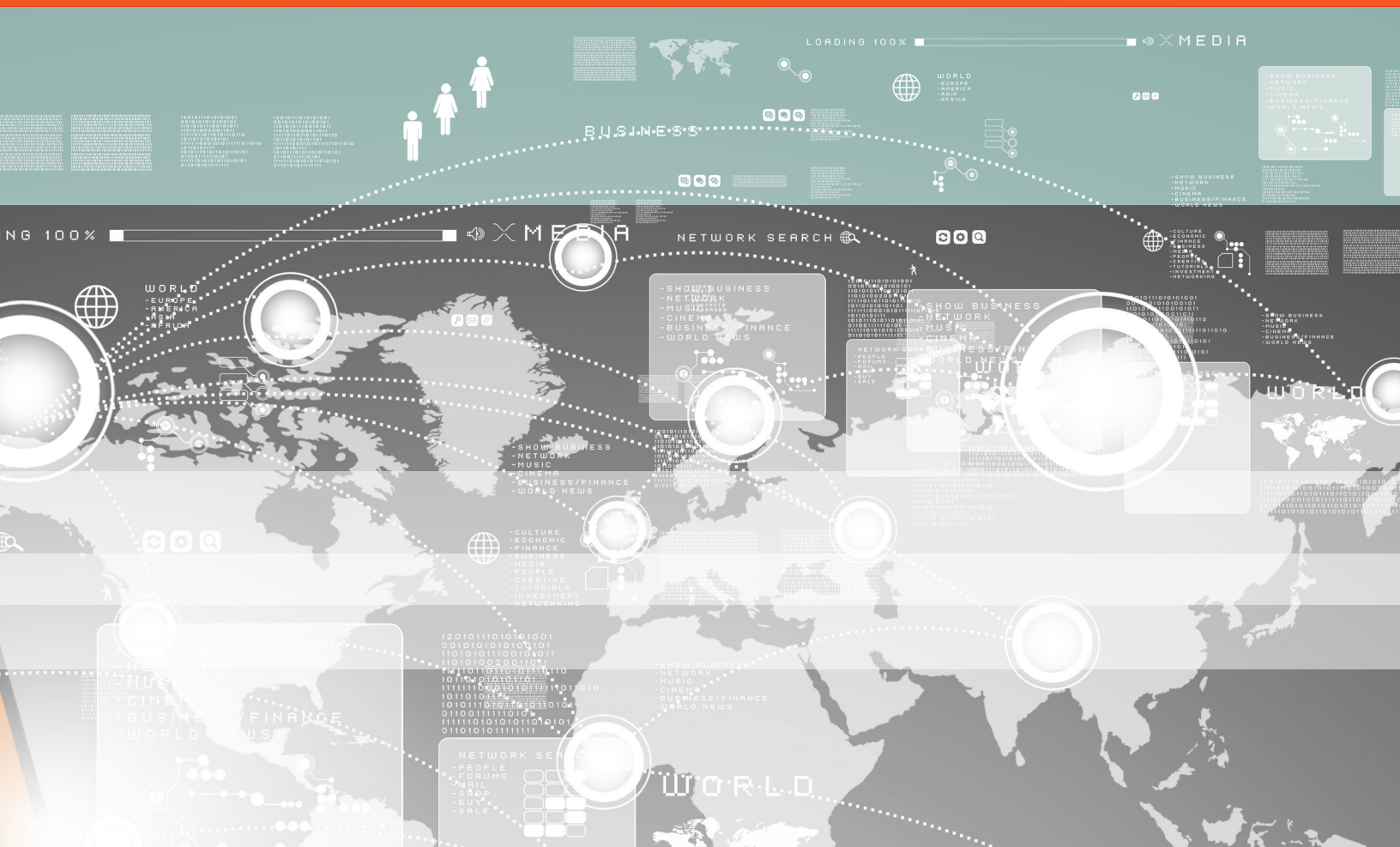
2019 Intelligent Authentication and Voice Biometrics Intelliview

opusresearch



opusresearch | Report »

2019 Intelligent Authentication and Voice Biometrics Intelliview »

In this report, Opus Research provides enterprise executives competitive context for 13 firms offering authentication solutions that include voice biometrics. In recent years, dramatic changes have taken place in both technology capabilities and market dynamics for voice biometrics solution providers. This document, including an appendix with a comprehensive list of company dossiers, provides a single point of reference to understand the competitive differences for companies offering software, services or platforms for voice-based authentication.

»

June 2019

Dan Miller, Lead Analyst & Founder, Opus Research

Opus Research, Inc.
350 Brannan St., Suite 340
San Francisco, CA 94107

www.opusresearch.net

Published June 2019 © Opus Research, Inc. All rights reserved.

Table of Contents

Appendix A - Company Dossiers

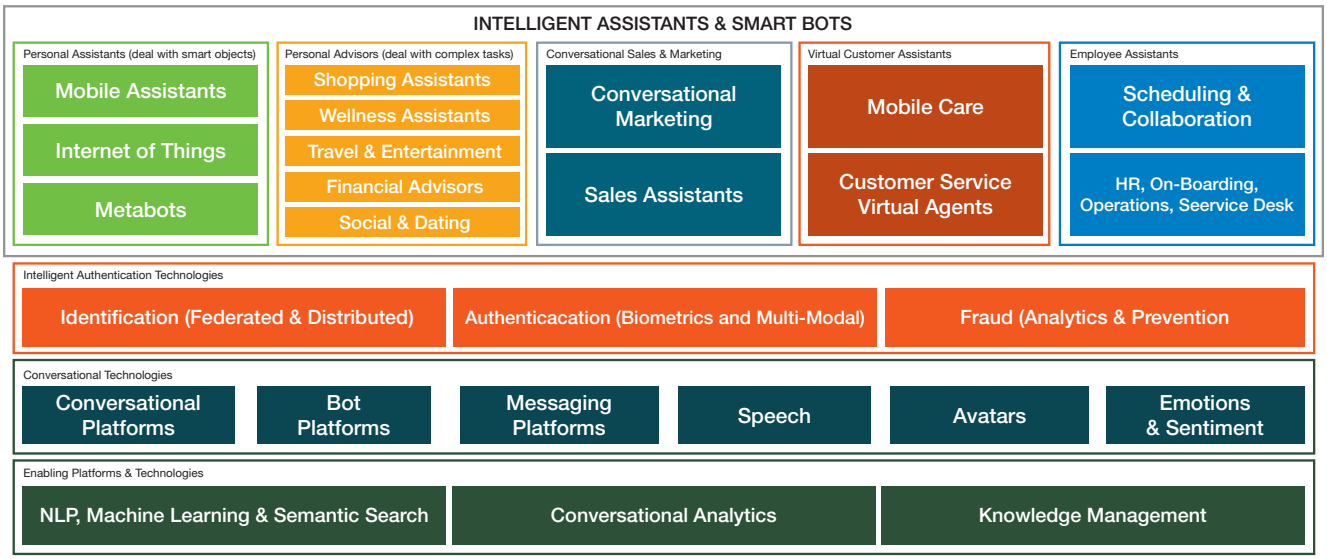
Table of Tables

The New Solution Stack for Intelligent Authentication (IAuth)

Brands across industries and around the world are establishing conversational engagement models with both customers and prospects. Large banks, financial services companies, e-retailers, wireless carriers and other global giants urge their best customers to download and use their mobile apps, add them to the contacts on their favorite messaging platform or engage through "chatbots" on their websites.

This triumph of Conversational Commerce is global in nature and expansive in terms of the vertical industries served. It has also surfaced the requirement for flavors of customer authentication that are effortless and continuous as well as foolproof. Opus Research, a technology analysis and marketing firm that specializes in conversational technologies, has long seen zero-effort authentication as a necessity for creating trusted links between brands and their customers. We've known it is a balancing act between security and convenience, which is why we looked to biometrics, specifically voice biometrics, as the foundation for simple assertion and authentication of a claimed identity in the context of a call to a customer care contact center.

Figure 1: Intelligent Assistance Solution Stack



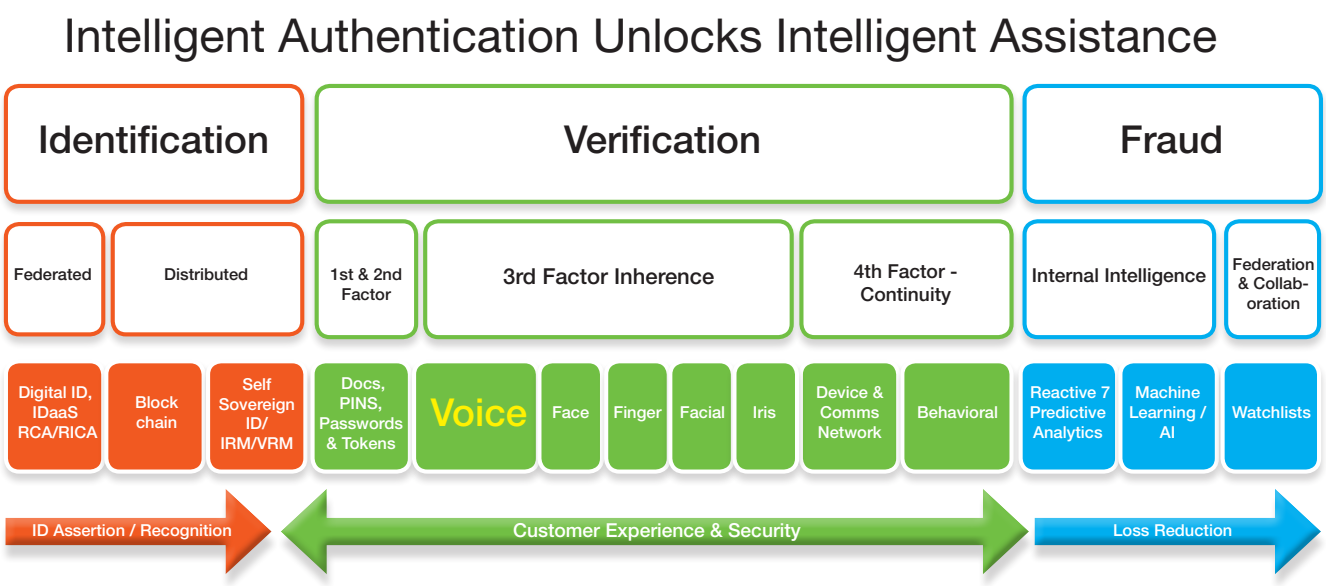
Source: Opus Research (2019)

In Figure 1, Opus Research depicts a layer of the Intelligent Assistance Solutions Stack called: "Intelligent Authentication." Intelligent Authentication Technologies rightfully reside between lower layers of Conversational Technologies and Platforms (which support bot creation, NLP, Machine Learning, Analytics and Knowledge Management) and the higher order functional blocks which, moving left to right, start with personal assistants like Siri, Alexa, Google Assistant and others and evolve into the sorts of advisors and agents that have specific expertise in financial services, travel & hospitality, healthcare and the like.

The Value of Voice

This document is the fourth in a periodic series of publications designed to help enterprise decision-makers understand Voice Biometrics (VB) technologies, solutions and vendors. The first Intelliview was issued in October 2013. At that time, VB was considered part of a point solution that enabled customer care contact center operators to use the unique aspects of each individual's voice to accelerate authentication and overcome long-standing dissatisfaction with so-called "Knowledge-Based Authentication" (KBA).

Figure 2: Where VB Fits into IAuth



Source: Opus Research (2019)

The ensuing years have witnessed consolidation among solutions providers and the addition of new entrants. The anticipated move to Communications Platforms as Service (CPaaS) is well underway. In support of Conversational Commerce, stalwart proponents of premises-based solutions for customer support and e-commerce among banks, brokerages, healthcare providers, government agencies and general e-commerce have been surprisingly swift to integrate cloud-based resources for analytics, natural language processing, machine learning and other cognitive resources. Intelligent Authentication (IAuth) is the next frontier.

A Word on Methodology

In early 2019, Opus Research circulated guidelines for candidates to provide input in the formatted dossiers that comprise Appendix A in this document. Our research team then applied the criteria described below in order to generate the Intelliview Map.

In this document, Opus Research evaluates 13 companies that offer group of solutions provides to define and fulfill on new requirements and grow the market. The list of attributes in a complete platform is lengthy and we applied both objective and subjective criteria to define where each candidate appears on the solution map.

Figure 3: Firms included in this report

Company	Emphasis
Aculab	API-based Virtual Appliance Approach
Auraya/ArmorVox	Global VB OEM
Interactions	VB integrated into Curo Intelligent Virtual Assistant
LumenVox	VoiceTrust plus USoft plus LumenVox
NICE Ltd.	Single enrollment, Passive enrollment and Auth
Nuance	Seamless, accurate authentication and fraud prevention
Omilia	DeepVB within DiaManT Platformj
Phonexia	VB integrated into data mining & speech analytics
Pindrop	Known for fraud prevention; Added VB, authentication
Sestek	Speech Processing
Spitch	Swiss-based, focus on work automation
Verint	Acquired VoiceVault for VB Auth
Verbio	Integrated VB into speech processing platform/suite

Source: Opus Research (2019)

New Intelliview Map: Selection Criteria for The Age of CPaaS

Solution providers have refined and redefined what comprises a complete solution set for voice biometrics-based products and services.

The primary criteria for inclusion are development, packaging and offering of a coherent VB-based solution. Historically, further factors for evaluation included:

Financial Strength: Longevity and known information regarding size of organization, customer base, investment in R&D, and profitability. Also pay attention to global scope and the ability to support multiple languages.

Overall Strategy and Vision: How does the solution provider see Voice Biometrics fitting into an overall Intelligent Authentication strategy and ultimately support multi-channel or optichannel Conversational Commerce.

Completeness of Product Offering: Both software and services across multiple deployment architectures.

- IVR, Contact Center, Mobile, multichannel
- Cloud, premises, embedded
- Enrollment Innovation: active, passive, opt-in/out, best practices for informed consent
- Authentication, Fraud Prevention, Device Activation

These criteria is more important than in previous editions because, in addition to integration with contact center and IVR resources, we are looking at the suitability for a layered defense for intelligent authentication and fraud prevention that embraces other biometric factors, including behavioral; additional non-biometrics (device), detect anomalies (network, channel, geography), anti-spoofing.

To assist decision makers in evaluating competing solutions providers, Opus Research places them on the Intelliview Map in positions that reflect their relative position based on the key criteria described below:

- **Seamless Authentication Across Multiple Modalities and Devices** - Streamline omnichannel customer authentication and stop fraudsters across all points of access.

- **Less Focus on Engines More on Results:** Most often been expressed in terms of false acceptance rates (FAR), letting an imposter through or false rejection rates (FRR) or blocking access to a legitimate customer voice is now one of many factors (biometric and other) that banks, brands and service providers use to support friction-free, risk- and context-aware authentication across a multiplicity of communications channels. As depicted in Figure 1 above, authentication solutions that include voice biometrics have, necessarily, changed and are no longer dedicated exclusively to voice biometrics-based solutions.

Positioning on the Intelliview Map

The criteria that Opus Research originally employed to support comparisons of market participants remain highly relevant, even though the meanings have, in all cases, shifted to put emphasis on a technology provider's ability to integrate into context-aware, multichannel environments.

The x-axis of the maps reflects "Market Position," which, looking exclusively at voice biometrics, reflects the success that the company has had in building an impressive roster of corporate customers and a correspondingly large number of enrolled "protected users" or a database of voiceprints.

The y-axis refers to "Breadth of Offering". In the original Intelliview (Opus Research, October 2013), this term referred almost exclusively to the robustness of voice processing capabilities, constrained to text-dependent authentication and imposter detection. Today, the wingspan of voice biometric-based offerings includes passive (text-independent) enrollment and authentication, integration with "risk engines" or other rules-based analytic resources that set thresholds based on massive amounts of contextual data and metadata.

The size of the ovals on the Intelliview reflect two, all-important factors:

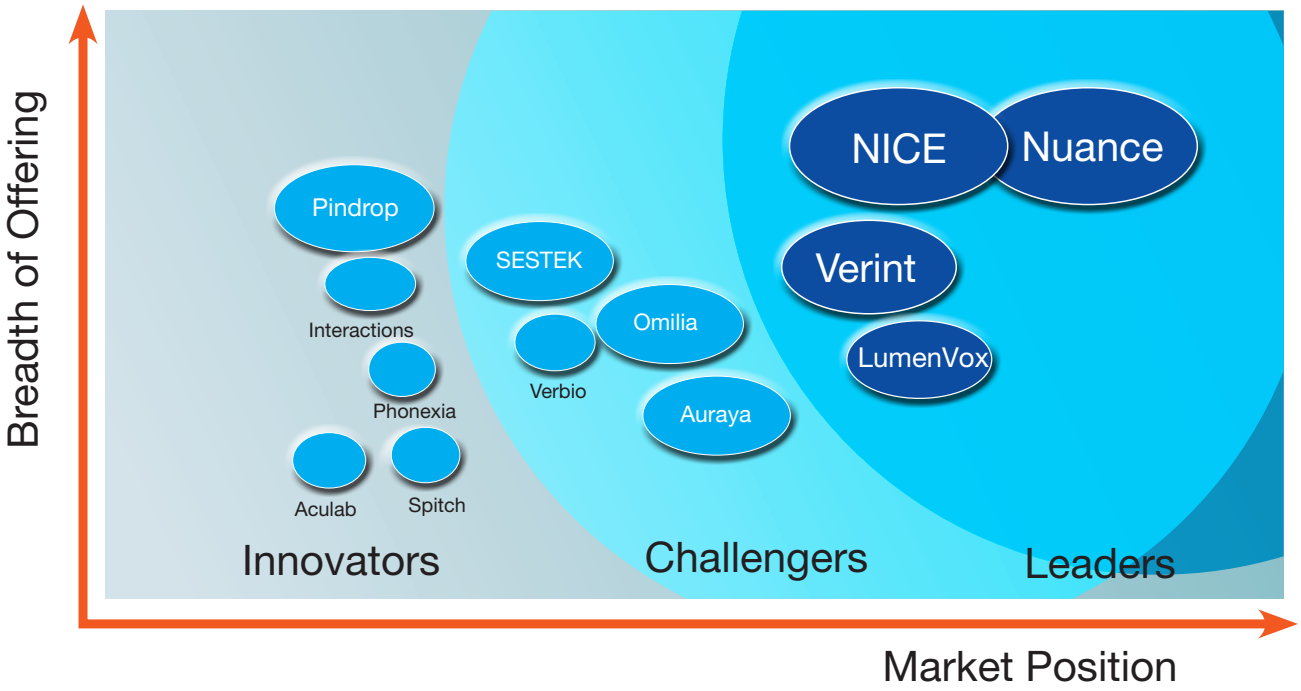
- **Financial Strength** – Solution providers in these secure, mission-critical environments must show staying power and the wherewithal to indemnify their customers should failure lead to fraud loss or have other negative impact on a company's reputation. In our dossiers, we pay attention to the longevity of a company, the size of its employee base and technical support staff and revenues (if available). All have an impact on

the company's ability to fulfill on commitments and all-important SLAs (Service Level Agreements).

- **Partnerships and Positioning** – This category takes on special importance as successful implementations reflect seamless integration with IVR, Contact Center, Web, Mobile and Digital Commerce software infrastructure. "Friction-free" authentication, interactions and transactions result from deep integration with existing resources that result from working relationships that are the product of strong business relationships.

As decision makers evaluate their options, they do so in the context of the explosive growth of digital commerce carried out over conversational platforms by a sophisticated set of customers. They seek holistic solutions that support "optichannel authentication", meaning that customers choose ("opt for") the best ("optimal") device or medium to support their present needs.

Figure 4: The Intelliview Map



Source: Opus Research (2019)

Excerpts of marketing material and narrative from each firm is contained in the lengthy appendix to this document.

To help with decision-making, here are a series of summaries of the vendor-provided material.

The Leaders

Nuance, **NICE**, **Verint** and **LumenVox** appear as leaders in the Intelliview Map based, primarily on the depth of products and services they offer. **Nuance** is the undisputed market share leader in terms of enrolled voiceprints associated with IVRs and contact centers as well as its self-described "multi-faceted, layered security approach that includes biometrics, non-biometric prints, anti-spoofing measures, intelligent detectors and pattern detection, employing AI techniques."

NICE packages voice biometrics as part of its broader offering of "Real Time Authentication", which leverages a leadership position in call recording with investment in voice biometrics and other core technologies to take "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." A key aspects of its approach is the ability to "passively" enroll protected customers by using existing recordings (with required consent, of course).

Nuance and **NICE** stand above in fulfilling the important basic need to support both active and passive voice-based authentication in contact centers.

Verint, like NICE, is a leader in call recording and, like LumenVox, has entered the broader Intelligent Authentication and Fraud domains through acquisition. It acquired Victrio in 2013 and more recently through acquisition of the intellectual property and customer base of VoiceVault. Voice biometrics is integrated into Verint's Real-Time Analytics Framework "of which, Identity Authentication and Real-Time Speech Analytics are the initial offering."

LumenVox enters the Leaders' ranks through the merger with VoiceTrust in late 2018. Since then it has stepped up investment in voice biometrics to complement its existing suite of automated speech processing resources, as well as a "unique workflow management-based approach" to support multifactor decisioning designed to enable a single deployment of its platform to support voice and facial authentication, fraud detection, and MFA in various configurations for multiple tenants.

The Challengers

The four solutions providers in the Challenger category are **Auraya, Omilia, Sestek** and **Verbio**.

Auraya's flagship product, Armorvox, is positioned as a platform primarily for use by third-party integrators to create universal voiceprints that can be used for active or passive authentication and fraud reduction in a broad variety of use cases.

Omilia, Sestek and Verbio offer broad suites of voice processing resources that treat voice authentication as a vital use case. Each has high-profile implementations, Turk Telecom in Turkey with Sestek, Omilia with banks and insurance companies in North America, and Verbio with large deployments in Spain and Latin America.

The Innovators

Pindrop tops the list here. The company is moving aggressively to apply investment a multiplicity of patents in deep neural networking (DNN) and artificial intelligence applied to fraud prevention to tackle both passphrase-based and passive authentication.

Interactions is a formidable innovator in terms of breadth of service. Voice biometrics is a key part of the Curo platform of speech processing technologies that was acquired from AT&T. It is in service for a large, unnamed telco.

Spitch offers Voice Biometrics as part of its enterprise-class conversational platform.

Phonexia Speech Platform makes VB part of a multi-factor authentication solution that seeks synergy from combining voice biometrics with speech analytics.

Aculab takes a decidedly innovative approach to brining voice-based authentication to both customer and employee facing implementations. It packages VoiSentry as an “appliance” or “virtual machine” that third-party developers can integrate into their phone-based customer care or employee help-desk applications.

The Path Forward: Simple, Secure, Trusted Conversations

Captured utterances reflect unique physical characteristics of the speaker’s vocal tract as well as unique attributes of how he or she says things. It is every bit as accurate as a fingerprint, facial scan, iris scan or other physical or behavioral qualities that are being employed to gain confidence that any individual is who he or she claims to be. Voice, however, should be the preferred biometric factor when conversations are taking place across voice channels. The firms under study in this report tell us that, in the aggregate they have enrolled roughly 600 million voiceprints that are put in service for over 2 billion authentications each year and reduced phone-based fraud losses by $300 billion.

The Leaders in this Intelliview, along with the Challengers and Innovators, provide their enterprise customers with solutions that take into account the following principles:

- Conversations replace “journeys” at the moment an individual establishes direct contact with a chosen brand.

- Zero-effort, conversational authentication is important to overcome the annoyance of PINs, passwords and KBAs.

- Authentication is key, not just for security and fraud reduction, but for personalization, privacy protection and customer control.
- To support zero-effort requires the introduction of "continuity" into the mix of authentication factors.
- Identity validation also takes on a position of importance to support trusted communication with new prospects.
- Biometrics have primacy because they are something you are, rather than something you know or something you have.
- Solutions that employ biometric-based authentication in conjunction with fraud detection and risk-based decision engines have proven both their economic and business value.

These principles define the way forward for solution providers and their enterprise customers. Collectively, they are bringing identification and access management into alignment with the way that people interact with businesses. In the context of heightened awareness about customer privacy and regulatory environments, individuals will have more tools to take charge of how they carry out conversations with their brands of choice.

Nuance Communications, Inc.

Headquarters: Burlington, MA (USA)
Total Number of employees: 9,000
Number of employees dedicated to R&D: ~2,000
Revenue: https://investors.nuance.com/investors/overview/default.aspx
Year of founding: 1992
www.nuance.com

Strategy & Vision:
Provide timeless, seamless, efficient and accurate authentication and fraud prevention through biometric, across devices and interaction channels. Here's a look at the future outlook for VB and Intelligent Authentication:

- There will be no more knowledge-based authentication: Nuance will deliver a comprehensive Security solution to address all Enterprise authentication and fraud prevention needs
- Biometrics will be the security standard to reliably validate who we are as consumers, citizens and employees: Nuance will offer a variety of biometric modalities to ensure complete coverage of an Enterprises' security requirements
- Security will be continuous and not a single step in a customer journey: Nuance will offer the end-to-end customer care experience that enables seamless security to consumers
- Fraudsters will focus their energies on spoofing biometrics as their primary attack vector: Nuance will continue to invest in core research, including the development of novel anti-spoofing technologies to stay ahead of emerging threats

Nuance is focussed on a multi-faceted, layered security approach that includes biometrics, non-biometric prints, anti-spoofing measures, intelligent detectors and pattern detection, employing AI techniques. The company is continually investing in research to improve VB engine, which is now in its 4th generation of DNNs, to be accurate with very short utterances such as individual words, which allows authentication for voice interfaces such as IVR, automobiles, TV, and IoT

devices. At the same time, ensuring a small engine footprint to run in embedded devices. Another important strategic area is the work being done on improving synthetic speech detection and spoofing attacks, which we believe will become an important threat to companies unable to detect these attacks.

Product Offerings

- Umbrella nomenclature or brand: Nuance Security Suite, Nuance Intelligent Engagement Platform
- Other authentication modalities (facial, behavioral, finger etc.)
  Facial recognition, Interaction behavioral biometrics, Conversational behavioral biometrics, device printing
- Sub-brands/components
  Text-dependent – active authentication
  Text-independent – passive authentication
  Fraud prevention
  Mobile SDK to support mobile authentication (embedded or connected)

Range of Services & Attributes

- ANI black list - Yes
- ANI spoofing detection - Yes
- IVR-based Authentication (Voice Captcha)- Yes
- Authentication of callers during live conversations with an agent
  - Speaker change detection - Yes
  - Continuous Authentication- Yes
  - Behavioral considerations- Yes
- Voice Identification - Yes
- Voice-based Liveness detection - Yes
- Anti-spoofing and Synthetic Speech Detection - Yes
- Mobile / Smartphone app authentication - Yes
  - Requires Internet connectivity or not? Support embedded, connected and Hybrid mode
- Password/Pin Reset - Yes
- Outbound call authentication (to validate a financial transaction for example) – Yes
- Proof-of-life - Yes
- Fraud Detection
  - Black list of voice prints - Yes
  - Black list of phone numbers - Yes

- Integration with other fraud and case management platforms – Yes, Enabled through our AI risk engine

Platform Attributes:

- Text Dependent Engine (Typical EER) – Under 1%
- Text Independent Engine (Typical EER) – Under 1%
- Can your product perform identification as well as verification? Yes
- Can the product perform both Text Dependent and Text Independent verification on a common Voiceprint - Yes
- Anti-spoofing (if yes, what technology)? Yes –Synthetic speech detection, playback detection, ANI spoofing detection, liveness detection,
- BOT/RAT, IVR BOT Detection, Velocity detection
- Server, on-device, hybrid or other architectures – we support all
- Do you have any certifications - Yes
  ISO 9001 (certification for the developing organization)
  ISO 27000 (certification for the developing organization under the aspects of security)
  TÜV Trusted Application Certificate

Unique Features

- **ConversationPrint** – A form of behavioral biometrics, identify individuals and fraudulent activity in real-time based on a choice of words and patterns of speech or writing during an interaction with a human or a virtual assistant. Analyze vocabulary, sentence structure, grammar, and more that are unique at an individual level

- **DevicePrint** – Non biometric print created for specific customer's device and can be compared to indicate potential fraudulent call

- **Passive Authentication in the IVR** – Nuance's newest generation of Deep Neural Networks can authenticate a caller passively in the IVR with as little as 0.5 seconds of audio, using their text-independent voiceprint created in the call center. Intelligent detectors – Comprehensive set of technologies that help identifying fraudsters. including channel identification, network identification and quality, geographical identification, ANI validation, ANI spoofing detection, IVR BOT detection, ANI velocity detection, gender detection, and several additional detection capabilities such as diarization, age, etc.

- AI Security Risk Engine – An engine that returns an authentication score and risk score based on multiple factors, modalities and inputs.

Delivery Model

- Direct, channel or both? Both, with over 200 sales rep
- Partners: Verint, Daon, IBM, Avaya, Genesys, Dimension Data, Red Box, Verizon, Diagenix, BT, KCOM, Accenture, Telstra, Presidio
- On prem, hosted or both (if both % of each)? Both (we do not break down % this way per our reporting process as a publicly traded company)
- Do you have a 'cloud-based' service? Yes
- Over 800 professional services staff

Pricing

- Tiered pricing, based on volume, per transaction – The tiered approach allows that the price adapts to the different sizes and volumes of the deployments being able to be competitive on small, medium and large size organizations.

Recommended Best Practices

If text dependent, what type of passphrase are recommended?
Recommend a phrase that is 1.5 seconds long with enough phoneme representation

Is Voice Biometrics linked to speech recognition?
While you do not need speech recognition for voice biometrics to work, recommend it as a best practice for text dependent solutions as well as liveness detection

How do you establish ground-truth in terms of establishing the identity of an individual when enrolled?
Designed to work around existing business processes for each institution. Best practice is to secure enrollment by ensuring that the agent is speaking to the true customer, or by adding a security factor in the IVR to secure self-service enrollment

Do you recommend opt-in or opt-out?
Opt-out will increase adoption rates for enrollment

How do you ensure PII protection?
A biometric print is a binary entity that represents the mathematical model of unique characteristics.

- Voiceprints/DevicePrints/ConvoPrints are stored in the Security Suite database and signed using a unique deployment ID
- Voiceprints/DevicePrints/ConvoPrints cannot be moved or transferred from server to server
- The biometric prints cannot be reverse engineered to produce the original audio used to train the biometric print.
- Most importantly, the biometric print cannot be tied back to the user

Preferred second factor when recommending Multi-Factor Authentication?
If using multi-factor authentication, and the first factor is a voiceprint, we recommend something other than a voiceprint such as DevicePrint for contact center, or faceprint for mobile etc.

Does your solution incorporate include additional factors including:

- Deep Neural Networks (DNN) – Yes, 4th generation
- Sentiment Analysis – N/A
- Keyword Spotting - Yes
- Language Identification - Yes
- Gender Identification - Yes
- Other – playback detection, synthetic speech detection, ANI spoofing, DevicePrint, facial recognition, behavioral biometrics, ConversationPrint

How would you link VB to growing interest in "Conversational AI"?
Nuance is a key player in the Conversational AI business and thanks to that, our Security business takes advantage of the synergies. Thanks to our 4th generation DNN technology that is able to authenticate the speaker with as low as 0.5s, we can fully integrate both functionalities, verifying the identity every time that you interact with your virtual assistant or bot.

Intellectual Property

In house technology; major version updates are released every year. Nuance has 65 issued patents in the field of voice biometrics, and many additional patents that are currently in the applications and review process.

Key Differentiators

- Comprehensive integrated authentication and fraud prevention solution across digital and voice channels – delivering end to end customer experience
- Industry leading authentication success rate and fraud prevention rate, outcome of continuous investment in core technology (including 4th generation DNN)
- Customers report better ROIs than organizations that deploy competing solutions, higher fraud loss savings and higher authentication success rates.
- Massive experience (20+ years) in deploying voice biometrics solution globally, ensuring our customers will derive the most value from the technology
- Unique features include ConverationPrint, Intelligent detectors, AI-based adaptation, AI-based risk decision, IVR DTMF BOT detection, ANI Call velocity detection and more.
- Nuance is the only company to provide 2 biometric modalities in the voice channel (voice biometrics + ConversationPrint)
- Nuance is the only company to provide 4 authentication modalities using 2 factors in the telephone channel (Voice Biometrics + ConversationPrint + DevicePrint + ANI validation)

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

This report shall be used solely for internal information purposes. Reproduction of this report without prior written permission is forbidden. Access to this report is limited to the license terms agreed to originally and any changes must be agreed upon in writing. The information contained herein has been obtained from sources believe to be reliable. However, Opus Research, Inc. accepts no responsibility whatsoever for the content or legality of the report. Opus Research, Inc. disclaims all warranties as to the accuracy, completeness or adequacy of such information. Further, Opus Research, Inc. shall have no liability for errors, omissions or inadequacies in the information contained herein or interpretations thereof. The opinions expressed herein may not necessarily coincide with the opinions and viewpoints of Opus Research, Inc. and are subject to change without notice.
Published June 2019 © Opus Research, Inc. All rights reserved.