NUANCE | WHAT'S NEXT BLOG

Customer engagement, Authentication & fraud prevention

The fraud landscape is rapidly evolving. So we're evolving voice authentication even faster.

Brett Beranek | Vice President & General Manager, Security & Biometrics

February 20, 2023

As fraudsters exploit new opportunities on digital channels, and contact center leaders strive to do more with less, many organizations are looking to voice biometrics to deliver more effective, efficient fraud prevention and customer authentication. But to successfully secure every channel, realize cost savings, and counter emerging threats, they need a solution that's both field-proven and cutting-edge.

They say necessity is the mother of invention. But it's also the mother of innovation. With a fraud landscape that's always evolving, intelligent fraud prevention solutions that evolve even faster are an absolute necessity.

At Nuance, our industry-leading research and development teams are constantly enhancing our security AI to stay ahead of modern threats. And in the past couple years, we've seen some seismic shifts.

As brands and their customers have embraced digital channels—from live chat to mobile apps—so have fraudsters. And in many instances, they've encountered weaker security and fresh opportunities. A professional fraudster, for example, can't hold five different telephone conversations at once. But they can run multiple simultaneous chat sessions from multiple devices, or even delegate this work to easily programmable bots.

This growing need to effectively secure omnichannel engagement is one factor driving organizations to

replace weak, knowledge-based authentication processes with voice biometrics. Another is the pressure born of challenging financial times.

Many contact center leaders are looking for ways to create more agile and efficient operations. They're turning to voice biometrics because of its potential to reduce average handle times, lighten the load on agents, and enable secure self-service for higher-risk customer interactions.

They need voice authentication solutions that don't just work on paper, but are proven to deliver these business outcomes in a production environment. They also need solutions that are highly accurate, so time isn't wasted on false fraud alerts and false customer rejects.

As voice biometrics become increasingly common, professional fraudsters have begun investing more time and resources into evading and duping the technology. While such techniques are still in their infancy, we've seen an increase in attempted attacks using synthetic and recorded speech—otherwise known as voice "deepfakes."

Why continuous innovation is essential

Deepfakes aren't a problem, and neither is the spike in digital fraud—*if* your voice biometrics solution is constantly evolving to detect these threats and keep you one step ahead.

Nuance pioneered active and passive voice biometrics in the early 2000s, and our solutions have consistently represented the bleeding edge of this technology. At the heart of our solutions is the Nuance Lightning Engine, a proprietary AI model that uses deep neural networks to authenticate customers and detect fraud across channels by analyzing the characteristics of the human voice.

With the latest and ninth generation of this engine, we've made significant enhancements that will help organizations strengthen their defenses, improve efficiency, and set the standard for the future of voice biometrics technology.

True omnichannel fraud prevention

Traditionally, the fidelity of voiceprints has been a barrier to using biometrics for authentication outside of the contact center. Not anymore.

Thanks to our latest improvements, a voiceprint captured through standard telephony can now be mapped to a high-fidelity model that supports seamless authentication in digital channels. That means once a customer has enrolled and created their voiceprint, they can use their voice for authentication in *any* channel—whether that's your IVR, mobile app, or website.

Streamlined operations and experiences

The Nuance Lightning Engine already delivered industry-leading speed, accuracy, and authentication success rates. We've continued to push the limits of what's possible to unlock even more efficient contact center operations and an even more streamlined customer experience.

Both enrolling and authenticating customer are now faster than ever. With a target authentication rate of 95%, for example, Nuance Lightning Engine can enroll customers based on as little as 5 seconds of audio, and authenticate them in half a second.

Supercharging our fraud detection capabilities

We've also elevated our AI model's intelligent fraud prevention capabilities to new heights.

Our exclusive biometric clustering feature allows fraud teams to identify previously unknown fraudsters by analyzing various aspects of call and chat interactions. With the latest generation of the Nuance Lightning Engine, you can now analyze tens of thousands of interactions in minutes, and get even more relevant and accurate results.

We've also succeeded in driving the engine's famously low error rates even lower, so you'll see even fewer false accepts and rejects that plague less sophisticated solutions.

And, of course, we've continued to strengthen the Nuance Lightning Engine's anti-spoofing capabilities, to bolster your organization's security posture in light of emerging threats. Our AI model is now even more effective at distinguishing live human speech from synthetic or recorded speech in real time—however sophisticated the attack.

Nuance has been collaborating with the Microsoft Cognitive AI research team throughout 2022 to fine-

tune our synthetic speech detection algorithm and provide customers with powerful real-time detection of artificial voices, such as those created by advanced generative AI models. Thanks to the dedication of our joint teams, we've improved the algorithm's detection rate to 86%. The addition of ConversationPrint, which analyses the linguistic patterns of an individual, increases the detection rate further to 99%.

The future of voice biometrics, available now

All these capabilities are available today. The Nuance Lightning Engine sits at the heart of our award-winning biometric security solution, Nuance Gatekeeper.

Nuance Gatekeeper is part of the Microsoft Digital Contact Center Platform, which uses AI and deep analytics to streamline service and increase satisfaction. But Gatekeeper is also cloud-native and platform-agnostic, working with leading Contact Center as a Service (CCaaS) offerings like Genesys, Avaya, Cisco, Five9, and Amazon Connect.

Simply put, we've built Gatekeeper to ensure you can benefit from the very best authentication and fraud prevention, whatever infrastructure and solutions you currently have in place.

Continuous innovation to combat constantly changing threats

It's exciting to see so many organizations looking to voice biometrics to prevent fraud across channels and realize efficiency gains in the contact center. But to hit those twin targets, you need solutions you know will deliver real-world outcomes *and* continuous innovation.

That's what our latest enhancements to Gatekeeper provide. They push our solution's industry-leading speed and accuracy rates even further, while unlocking truly omnichannel fraud prevention and shutting the door against emerging threats.

Want to explore the other trends that we can see reshaping the contact center? Check out Tony Lorentzen's customer engagement predictions for 2023.

Tags: Contact center strategy, Nuance Gatekeeper, Predictions, Synthetic voice detection, Deepfakes

More Information

Meet Nuance Gatekeeper

Find out how you can protect your customers and your business, with cloud-native biometric security for every channel.

Learn more

About Brett Beranek

Brett Beranek is responsible for overseeing the security and biometric line of business at Nuance, a Microsoft company. In this role for the past 12 years, Beranek has brought Nuance to a leadership position in the biometric authentication and biometric fraud prevention space. A thought leader in the field of biometrics, Beranek is a frequent contributor in industry events and the media on the topic of AI technology and it's use by the fraud community, and how society can mitigate against these evolving threats. Prior to Nuance, he held various leadership positions in the biometrics and security industry. He has earned a Bachelor of Commerce, Information Systems Major, from McGill University as well as an Executive Marketing certificate from Massachusetts Institute of Technology's Sloan School of Management. Beranek is also a certified Master Fraud Prevention Black Belt professional.

View all posts by Brett Beranek