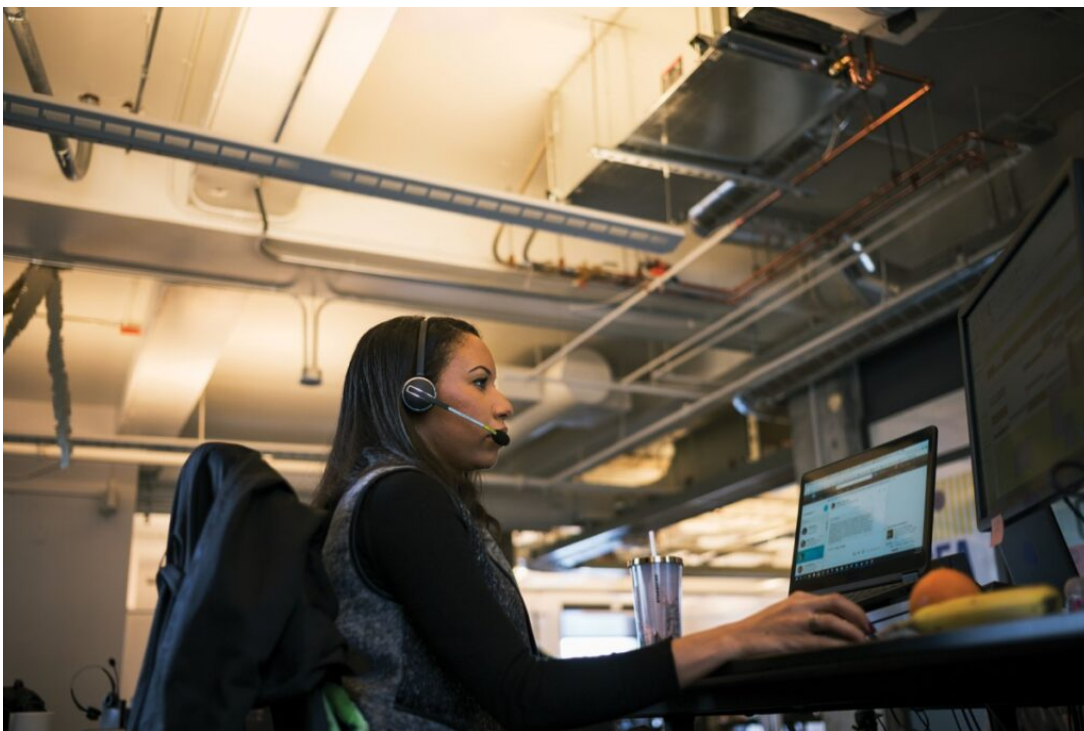**NUANCE** | **WHAT'S NEXT BLOG**

Customer engagement, Contact Center AI

The AI-powered contact center, part 4: Enhance contact center security with biometric authentication

Tony Lorentzen | General Manager & Senior Vice President, Intelligent Engagement

August 30, 2022

Advanced biometric security solution that streamlines customer engagements and protects interactions in every channel. We look at how integrating Nuance Gatekeeper with Microsoft innovations on the Microsoft Digital Contact Center Platform helps enhance customer experiences and improve fraud prevention.

This was originally published on Microsoft.com on August 29, 2022.

When a customer needs support, they not only expect fast, convenient ways to get help, but also to have their personal information protected. However, when verifying that people are who they say they are, many contact centers use traditional authentication methods are no longer fit for purpose. That's why the biometric security on the Microsoft Digital Contact Center Platform is so essential—with biometrics, contact centers can provide intelligent fraud prevention and fast, effortless customer authentication.

Why contact center security must change

The classic methods for verifying customer identities and weeding out fraudsters depend on knowledge-based authentication (KBA)—the PINs, passwords, and security questions we are all familiar with. However, KBA causes problems in multiple ways:

1. It's very easy for fraudsters to steal, buy, or phish for customers' information, which makes it simple for them to pass KBA checks.
2. Lengthy authentication processes add friction to the customer journey—and often must be performed multiple times as customers move between channels.
3. Customers expect brands to know who they are; they don't want to sit through an interrogation to prove their identity.
4. Customers often lose or forget the authentication information they need, increasing the time, effort, and frustration of the interaction as they search for usernames and passwords.

That is why biometric security is so important for helping organizations protect their customers and their business.

With biometrics, organizations can leave the issues of KBA in the past by enabling fast, frictionless, and accurate authentication for genuine customers while quickly detecting fraudsters and preventing fraud in every channel.

By layering voice, behavioral, and conversational biometrics (how people sound, how they behave, and what they say) with non-biometric factors, a central AI risk engine can make intelligent assessments of authentication and fraud risk. By using biometrics, the system can identify the actual person behind the interaction, rather than just the information they have or the device they are using.

And now that Nuance Gatekeeper biometric security is closely integrated with Microsoft products on the Microsoft Digital Contact Center Platform, our combined solutions will multiply the benefits for all our customers.

Seamless authentication

The combination of Gatekeeper and Microsoft Dynamics 365 Customer Service on the Digital Contact Center Platform will help strengthen the overall identification and verification (ID&V) process and give agents tools that help them provide seamless service across any channel. While customer relationship management (CRM) data provides the customer ID, multimodal biometrics bolsters verification to validate customer identities quickly and accurately. Meanwhile, call validation detects common fraud tactics like Automatic Number Identification (ANI) spoofing, and environment detection interrogates the trustworthiness of device and network signals.

Stronger fraud prevention

As stated earlier, biometric security has a dramatic impact on organizations' ability to detect and prevent fraud in customer engagements across any channel. Dynamics 365 Fraud Protection is a perfect complement to biometrics—providing an adaptive AI tool that guards organizations against payment fraud, account takeovers, and many other transactional fraud threats.

With these technologies working in unison, the AI has an enriched data set to make better-informed decisions about when to use step-up authentication or flag a transaction or individual as suspicious. Gatekeeper identifies the human behind the transaction while Dynamics 365 examines the transaction itself—a powerful combination that delivers a unique offering in the fraud protection market.

Enhanced personalization

With biometric authentication, it is also much simpler to personalize customer engagements from the beginning; particularly with passive voice biometrics, where customers can be identified and their experience tailored within seconds as they explain their need to an agent or a conversational interactive voice response (IVR).

Voice biometrics solutions make it simpler to offer personalized service and specialized support to a variety of customers. For example, Telefónica, the leading Spanish telco, needed a way to prioritize vulnerable customers at the start of the pandemic, when call volumes skyrocketed. It used voice biometrics to identify seniors based on numerous voice characteristics and route them directly to a priority service line, offering a more personalized experience for seniors who depend on Telefónica to keep them connected.

There is also an opportunity to create more personalized experiences for employees. Another exciting benefit of bringing Nuance and Microsoft products together on the Digital Contact Center Platform is the integration between Gatekeeper and Azure Active Directory (Azure AD). Employees at many enterprises across the globe use Azure AD to log into their accounts every day, and that will become even simpler by using biometric authentication instead of usernames and passwords.

Create a more secure contact center

Our vision for the future of the digital contact center is one where biometric security is built into all customer engagements to streamline, personalize, and protect every interaction.

By integrating our products on a single platform, we are bringing that vision to life, empowering customer engagement teams to serve and sell more effectively and enabling fraud teams to detect and prevent more fraud.

Learn more about our contact center solution

Throughout this series, we have explored how to create engaging, personalized digital experiences, achieve superior self-service voice support, and build conversational AI applications with the protection of advanced biometric security solutions. This is the contact center of the future, made possible with the Microsoft Digital Contact Center Platform.

Tags: Contact center strategy, Nuance Gatekeeper, Microsoft + Nuance

More Information

The Microsoft Digital Contact Center

Discover how Nuance, Dynamics 365, and Microsoft Teams could shape the future of your contact center.

Learn more

About Tony Lorentzen

Tony has more than 25 years of experience in the technology sector, spending the last 17 with Nuance where he is currently the SVP of Intelligent Engagement Solutions within the Enterprise Division. Before that he served as the leader of several teams at Nuance including Sales Engineering, Business Consulting, and Product Management. A proven leader in working with the cross-functional teams, Tony blends his in-depth knowledge of business management, technology and vertical domain expertise to bring Nuance's solutions to the Enterprise market, partnering with customers to ensure implementations drive true ROI. Prior to Nuance, Tony spent time at Lucent and Verizon where he led teams that applied the latest technologies to solve complex business issues for large enterprises. Tony received a B.S. from Villanova University and a MBA from Dowling College.

View all posts by Tony Lorentzen