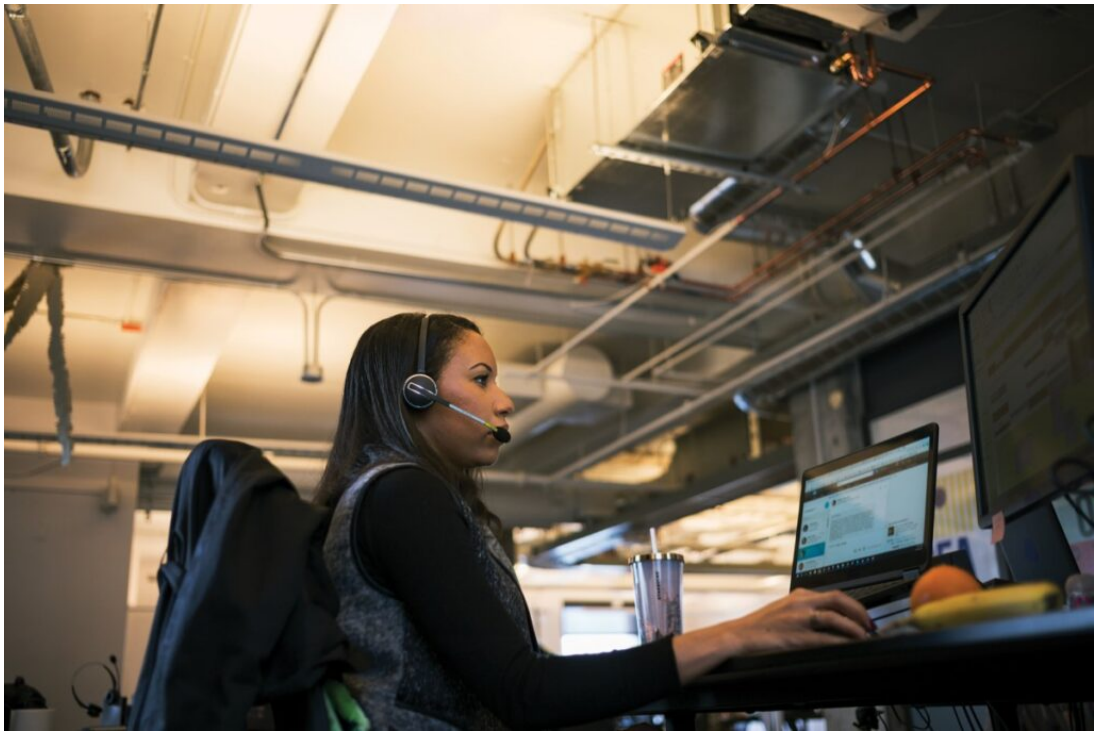
NUANCE | WHAT'S NEXT BLOG

IA para Contact Centers, Interacción con el cliente multicanal

El contact center impulsado por la IA, parte 4: Mejorar la seguridad del contact center con la autenticación biométrica

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

25 enero 2023



Solución de seguridad biométrica avanzada para verificar la identidad de los clientes de forma rápida, fácil y segura, y proteger las interacciones en todos los canales. Examinamos cómo la integración de Nuance Gatekeeper con las innovaciones de Microsoft en la plataforma Microsoft Digital Contact Center, ayuda a mejorar la experiencia de los clientes y a detectar el fraude.

Este blog se publicó originalmente, en inglés, *en Microsoft.com.*

Cuando un cliente necesita asistencia, no sólo espera una forma rápida y cómoda de obtener ayuda, sino también que se proteja su información personal. Sin embargo, a la hora de verificar que las personas son quienes dicen ser, muchos contact centers utilizan métodos de autenticación tradicionales que ya no son adecuados para su propósito. Por ello, las soluciones de seguridad biométrica incluidas en la plataforma de contact center digital de Microsoft son esenciales. Gracias a la biometría, todo tipo de organizaciones pueden verificar la identidad de sus clientes de forma rápida, fácil y segura en todos los canales, para operar con total tranquilidad y protegerse contra el fraude.

Por qué hay que reforzar la seguridad en los contact centers

Los métodos tradicionales para verificar la identidad de los clientes han quedado obsoletos, son vulnerables y añaden fricción. A punto de comenzar el 2023, los métodos de autenticación aún dependen de la autenticación basada en el conocimiento (KBA), es decir, de los PIN, las contraseñas y las preguntas de seguridad que todos conocemos. Tienen que evolucionar:

1. Para los criminales es muy fácil conseguir información personal de los clientes y suplantar su identidad. Nuestras contraseñas e información personal están expuestas en internet, en distintas plataformas y redes. Además, no podemos olvidar que estamos tratando con verdaderas bandas de cibercrimen organizado. Son profesionales y tienen los recursos y formación necesarios para llevar a cabo un delito sin demasiada dificultad, con este tipo de métodos de autenticación.
2. Los largos procesos de autenticación añaden fricción y una mala experiencia. Además, tenemos que autenticarnos en repetidas ocasiones dentro la misma cuenta cuando pasamos de un canal a otro, o simplemente queremos realizar una nueva operación.
3. Los clientes esperan que las marcas sepan quiénes son desde el primer instante que se ponen en contacto con sus empresas, y no quieren someterse a un interrogatorio para demostrar su identidad.
4. Los clientes a menudo pierden u olvidan la información que necesitan para ser autenticados. Lo que aumenta el tiempo de poder acceder a cualquier consulta u operativa, supone un esfuerzo adicional por ambos lados (empresa y cliente) y la correspondiente frustración al no poder resolver la consulta de forma inmediata por culpa de una contraseña o un protocolo de seguridad ineficiente.

Por eso la seguridad biométrica es tan importante para ayudar a las organizaciones a **proteger a sus clientes y sus propios negocios.**

Con la biometría, las organizaciones pueden ser **más eficientes** y dejar los problemas de los métodos tradicionales de autenticación basados en el conocimiento al permitir una autenticación rápida, segura y sin fricciones, garantizando que las personas con las que interactuamos son realmente quienes dicen ser.

Utilizando elementos biométricos inherentes como la biometría de voz, el comportamiento y la biometría conversacional (cómo suenan las personas, cómo se comportan y lo que dicen) con factores no biométricos, un motor de riesgo de IA central puede hacer evaluaciones inteligentes del riesgo de autenticación y fraude. Al utilizar la biometría, el sistema puede identificar a la persona real que está detrás de la interacción, en lugar de limitarse a la información que tiene o al dispositivo que utiliza.

Y ahora que la seguridad biométrica de Nuance Gatekeeper está integrada con los productos de Microsoft en la plataforma Microsoft Digital Contact Center, nuestras soluciones multiplicarán las ventajas para todos nuestros clientes.

Autenticación sin interrupciones

La combinación de Gatekeeper y Microsoft Dynamics 365 Customer Service en la plataforma de contact center digital ayudará a evolucionar y reforzar la seguridad de los procesos de identificación y verificación (ID&V) y a proporcionar a los agentes y empleados herramientas que les ayuden a prestar un servicio sin interrupciones en cualquier canal. Mientras que los datos de gestión de las relaciones con los clientes (CRM) proporcionan la identificación del cliente, la biometría multimodal refuerza la verificación para validar la identidad de los clientes con rapidez y precisión.

Por su parte, la validación de llamadas detecta tácticas de fraude habituales, como la suplantación de la identificación automática del número (ANI), y la detección del entorno, cuestionando la fiabilidad de las señales del tipo de dispositivo y la red.

Mayor detección y prevención del fraude

Como hemos dicho anteriormente, la seguridad biométrica tiene un impacto espectacular en la capacidad de las organizaciones para detectar y prevenir el fraude durante las interacciones con los clientes a través de cualquier canal. Dynamics 365 Fraud Protection es un complemento perfecto para la biometría, ya que proporciona una herramienta de IA adaptativa que protege a las organizaciones contra el fraude en los pagos, suplantación de identidades, apropiación indebida de cuentas y muchas otras amenazas de fraude transaccional.

Con estas tecnologías trabajando al unísono, la IA dispone de un conjunto de datos enriquecidos para

tomar decisiones mejor informadas sobre cuándo utilizar la autenticación escalonada o marcar una transacción o individuo como sospechoso. Gatekeeper identifica a la persona que está detrás de la transacción, mientras que Dynamics 365 examina la transacción en sí. Una potente combinación que ofrece una oferta única en el mercado de la protección contra el fraude.

Potenciando la personalización

Con la autenticación biométrica, también es mucho más sencillo personalizar las relaciones con los clientes desde el principio. En particular, con la biometría de voz pasiva, donde los clientes pueden ser identificados y su experiencia adaptada en cuestión de segundos mientras explican su necesidad a un agente, un sistema IVR o un asistente virtual.

Las soluciones de biometría de voz simplifican la tarea de ofrecer un servicio personalizado y una asistencia especializada a diversos clientes. Por ejemplo, Telefónica necesitaba encontrar la forma de priorizar la atención de los clientes mayores de 65 años, más vulnerables durante la pandemia, cuando el volumen de llamadas se disparó de tal forma que resultaba imposible priorizar la atención de las personas más necesitadas. **Telefónica utilizó la biometría de voz para identificar a las personas mayores de 65** en función de numerosas características propias de la voz y pudo dirigirlas directamente a una línea de servicio prioritario.

También existe la oportunidad de crear experiencias más personalizadas para los empleados. Otro beneficio interesante de unir los productos de Nuance y Microsoft en la plataforma digital de contact center es la integración entre Gatekeeper y **Azure Active Directory** (Azure AD). Los empleados de muchas empresas de todo el mundo utilizan Azure AD para iniciar sesión en sus cuentas cada día, y eso será aún más sencillo al utilizar la autenticación biométrica en lugar de nombres de usuario y contraseñas.

Crear un contact center más seguro

Nuestra visión del contact center digital incorpora la seguridad biométrica en todas las interacciones con los clientes para agilizar, personalizar y proteger cada conversación, consulta u operación en todos los canales. Al integrar nuestros productos en una única plataforma, estamos haciendo realidad esa visión, permitiendo a los equipos y departamentos de atención al cliente dar mejor soporte y vender más y mejor, y a los equipos de fraude detectar y prevenir más fraude.

Más información sobre nuestra solución de contact center

A lo largo de esta serie de artículos, hemos explorado cómo **crear experiencias digitales atractivas y personalizadas, lograr un autoservicio mediante soluciones de voz superior** y **crear aplicaciones de IA conversacional** con la protección de soluciones de seguridad biométricas avanzadas. Este es el contact center del futuro, que es posible gracias a la plataforma de **contact center digital de Microsoft.**

Tags: Fraude, Seguridad y biometria, Plataforma de Contact Center Digital de Microsoft

More Information

Más información

Descubre como Nuance, Dynamics 365 y Microsoft Teams puedan dar forma al futuro de tu contact center.

Learn more

About Tony Lorentzen

Tony, que cuenta con más de 25 años de experiencia en el sector tecnológico, trabaja en Nuance desde hace 17, donde es vicepresidente de Intelligent Engagement Solutions dentro de la división Enterprise. Previamente lideró varios equipos en la compañía, incluyendo Ingeniería de Ventas, Consultoría de Negocio y Product Management. Con su experiencia, Tony lleva las soluciones de Nuance al mercado empresarial, asociándose con los clientes para garantizar que las implementaciones generen un verdadero retorno de la inversión. Antes de Nuance, trabajó en Lucent y Verizon, donde dirigió equipos que aplicaban las últimas tecnologías para resolver problemas empresariales complejos. Tony se licenció en la Universidad de Villanova y obtuvo un MBA en el Dowling College.

View all posts by Tony Lorentzen