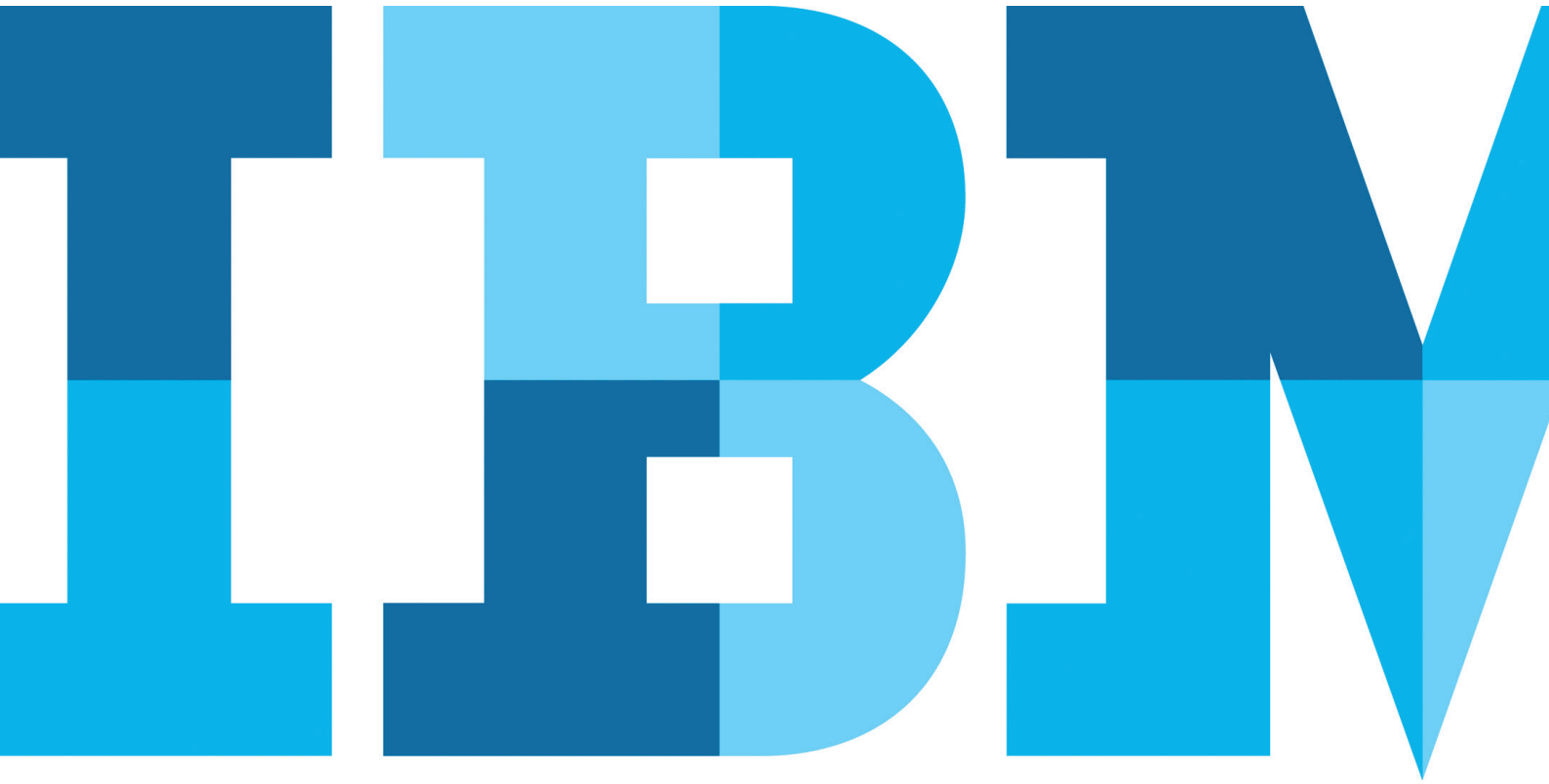
Creación de una experiencia digital fluida para los clientes de seguros

IBM Trusteer ayuda a las aseguradoras a evaluar de manera transparente los riesgos de la identidad digital



IBM

Contenido

Introducción

Hubo una época en la que el principal canal de las aseguradoras para interactuar con los clientes era a través de sus profesionales de seguros (también conocidos como agentes de seguros). Si bien los profesionales de seguros aún juegan un papel importante en la experiencia del cliente, el mercado de seguros, como muchas otras industrias, está aumentando el uso de los canales digitales de bajo costo para conectarse mejor con los usuarios externos y llegar a nuevos mercados.

En los últimos años, las aseguradoras han implementado aplicaciones digitales que permiten a los consumidores verificar la información de la póliza, revisar los beneficios, comparar costos, pagar facturas, iniciar reclamos e incluso solicitar cobertura desde sus teléfonos móviles o computadoras de escritorio. Este esfuerzo de transformación reduce el costo del servicio al cliente, al tiempo que genera nuevas oportunidades para acercarse a los clientes y fortalecer la lealtad a la marca.

A medida que continúa la transformación digital, las aseguradoras apuntan a ampliar las ventas con nuevos productos de seguros diseñados para el canal digital, ya sea entregados directamente a través de sus sitios o a través de socios que utilizan interfaces de programación de aplicaciones (API).

Las aseguradoras también han invertido en agilizar los procesos y servicios con proveedores externos que administran servicios de resolución de reclamaciones (por ejemplo, médicos, empresas de reparación de viviendas, empresas de reparación de parabrisas de automóviles). Este trabajo puede ayudar a las aseguradoras a ofrecer servicios de resolución de reclamaciones a los clientes y atraer a más proveedores para que trabajen con la aseguradora.

Sin embargo, crear una experiencia digital fluida para consumidores, proveedores y profesionales de seguros puede ser un desafío.

Los consumidores, proveedores y profesionales de seguros de hoy en día esperan conveniencia, tanto en términos de facilidad en el uso de servicios digitales como en la capacidad de recibir atención en cualquier momento y desde cualquier lugar. Una gran cantidad de pasos (ya se trate de demasiados pasos para la autenticación o de demasiados formularios para ser enviados digitalmente o a través de un profesional de seguros) puede ser percibida por el usuario como onerosa. Dicha complejidad en los procesos puede afectar la experiencia digital del usuario y, en última instancia, dar como resultado una alta tasa de abandono en la que consumidores, proveedores y profesionales de seguros recurren a canales más caros, como el centro de llamadas, o acuden a otra aseguradora.

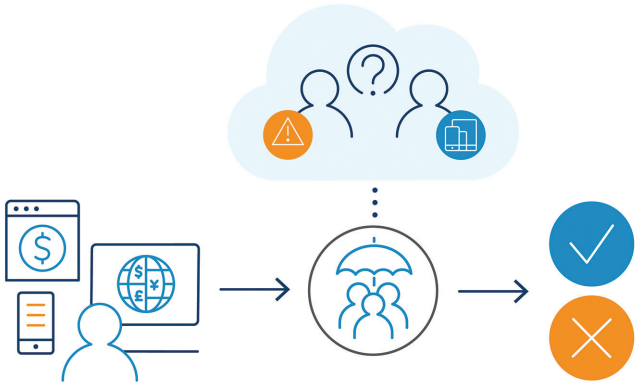
En esta era digital, los consumidores tienen el poder, con solo tocar una pantalla, para comparar precios y ofertas, e incluso dictar cómo y cuándo quieren hacer negocios con la aseguradora.

La reputación por un servicio al cliente deficiente o por una falla en la seguridad, puede tener un impacto significativo en esta industria altamente competitiva. Además, una cuenta digital comprometida de un proveedor o profesional de seguros puede representar un alto riesgo para la aseguradora, ya que una cuenta de reclamos puede usarse para presentar cientos de reclamos o generar pólizas de bajo costo.

Entonces, la pregunta es: ¿cómo puede usted establecer confianza a través de los canales digitales para poder acoger fluidamente tanto a clientes nuevos como existentes, así como a proveedores y profesionales de seguros, al tiempo que mantiene alejados a los infiltrados?

La respuesta está en cómo evalúa el riesgo de las identidades digitales.

Para ayudar a identificar de manera transparente a los verdaderos usuarios en el canal digital y ayudar a detectar posibles infiltrados con mayor precisión, las aseguradoras necesitan una sólida capacidad de evaluación de riesgos de identidad digital para examinar las huellas digitales de cada usuario a partir de varias entradas sensoriales de la máquina.



¿Cómo puede recibir fluidamente a los clientes mientras mantiene alejados a los infiltrados?

El valor de las evaluaciones de riesgo sólidas

A continuación se enumeran cuatro beneficios potenciales de realizar evaluaciones de riesgo sólidas al comienzo de cualquier interacción digital (ya sea un nuevo cliente que solicita una póliza, un cliente existente que utiliza el canal digital en lugar de un canal tradicional, o un proveedor que inicia sesión para enviar nuevos reclamos).

Brinde una experiencia de usuario más fluida

En primer lugar, la realización de evaluaciones sólidas de riesgos de identidad digital puede ayudarle a brindar una experiencia más fluida a los usuarios existentes cada vez que ellos inicien sesión en sus cuentas. Con la autenticación continua basada en el riesgo, en lugar de sobrecargar a los usuarios con múltiples protocolos de autenticación en cada inicio de sesión, usted tiene información que le permite cuestionar solo a aquellos usuarios con un alto riesgo de intención maliciosa. Además, mediante la autenticación continua, puede evaluar a los usuarios cuando estén a punto de realizar una operación altamente confidencial, revalidando así la confianza y el riesgo solo cuando sea necesario. Las aseguradoras que ofrecen una experiencia digital deficiente, con fricción adicional en la autenticación, pueden, en última instancia, enfrentar la migración de los usuarios de servicios digitales a la competencia o canales de mayor costo.

Una experiencia más fluida también puede ayudar a las aseguradoras a aumentar los puntajes de fidelidad de los clientes. A menudo, el uso del canal digital por parte de un cliente existente se presenta debido a un evento estresante de la vida: un accidente automovilístico, una enfermedad o la muerte de un ser querido. Es posible que algunos de estos clientes no inicien sesión en sus cuentas de manera regular y, como resultado, es más probable que tengan problemas con un proceso de autenticación complejo o contraseñas olvidadas. Al facilitar el proceso, las aseguradoras pueden demostrar su compromiso de ayudar a los clientes a superar los desafíos de la vida y aprovechar estos momentos como una oportunidad para generar una mayor lealtad a la marca. Para un proveedor o profesional de seguros, cada minuto dedicado a la autenticación puede significar la pérdida de ingresos por atender reclamos adicionales. Reducir los desafíos de autenticación sin comprometer la seguridad puede contribuir en gran medida a mantener la fidelidad de los clientes y la preferencia de hacer negocios con la aseguradora.

Ayude a ganar y retener clientes

En segundo lugar, la realización de evaluaciones puede ayudar a las aseguradoras a ganar y retener clientes. Las comprobaciones de autenticación excesivas son un impedimento significativo para los consumidores que desean la libertad de comprar una nueva cobertura en cualquier momento y en cualquier lugar. Si les pone demasiados obstáculos para demostrar que son quienes dicen que son, es posible que busquen otras aseguradoras que puedan brindarles esa experiencia sin demoras, que ellos demandan.

Ayude a proteger los datos de los clientes

En tercer lugar, la realización de evaluaciones puede respaldar iniciativas de políticas y riesgo para ayudar a proteger los datos de los clientes. Los ciberdelincuentes han ideado muchas maneras de eludir los procesos de autenticación, incluida la autenticación de dos factores, para suplantar a los usuarios. Una cuenta comprometida de un proveedor o profesional de seguros puede exponer los datos de cientos de clientes a un infiltrado. Las evaluaciones

sólidas de riesgos de identidad digital que utilizan autenticación pasiva pueden ayudar a descubrir patrones ocultos que indican que el usuario que inicia sesión no es un cliente, proveedor o profesional de seguros legítimo, sino un infiltrado que ha obtenido las credenciales del usuario.

Ayude a reducir el impacto operativo

Finalmente, las evaluaciones sólidas de riesgos de identidad digital pueden ayudar a reducir el impacto operativo de los intentos maliciosos. Al detener a los infiltrados al inicio de una interacción digital, las aseguradoras pueden reducir potencialmente el costo de las investigaciones y procesamientos manuales, así como evitar la necesidad de enviar cartas de explicación de un rechazo o manejar los costos extensos de una vulneración de datos. Las herramientas heredadas con tecnologías anticuadas, a menudo requieren una excesiva y continua interacción humana. Las estrategias basadas en la inteligencia adaptativa, que aprovechan más la automatización y disminuyen la dependencia en la participación humana, pueden ayudar a aumentar la precisión a escala, al tiempo que reducen el riesgo de fraude y los costos operativos.

Consideraciones en la evaluación de las identidades digitales

Uno de los desafíos al evaluar eficazmente las identidades digitales es que las aseguradoras enfrentan muchas amenazas en evolución en el panorama digital.

Los diferentes tipos de delitos son cometidos por diferentes tipos de infiltrados en diferentes etapas del ciclo de vida de la interacción del usuario, desde la compra de seguros hasta la presentación de reclamos y la prestación de servicio al cliente. Las tácticas pueden incluir:

- Crear identidades falsas o sintéticas (identidades que incorporan datos robados o agregan datos falsos a identidades reales) para el fraude de propios y terceros.
- Usar identidades reales pero robadas, un problema creciente dado el alcance de la información de los usuarios —como nombres, direcciones, fechas de nacimiento, segundos nombres y números de seguro social— que se ha visto comprometida por vulneraciones de datos.
- Hacerse pasar por clientes, proveedores o profesionales de seguros existentes para hacer reclamos, recibir pagos, liquidar o solicitar préstamos sobre una póliza, o simplemente robar los datos de los clientes.
- Comprar repetidamente seguros de diferentes aseguradoras solo para presentar un reclamo y obtener un pago.

Como resultado, cuantos más datos pueda incorporar en sus evaluaciones de riesgo, mayor será la precisión de sus alertas. Una mayor precisión puede ayudar a reducir los costos operativos y generar menos falsos positivos para el equipo de fraudes.

Por lo tanto, las aseguradoras deben considerar una amplia gama de datos al evaluar la legitimidad de cada usuario. Esto incluye:

- Autenticidad del dispositivo y evidencia de suplantación de identidad para ayudar a mejorar la confiabilidad de las huellas digitales del dispositivo. Las huellas digitales de los dispositivos y la asociación de los dispositivos con los usuarios pueden respaldar una autenticación transparente. Sin embargo, debido a que los infiltrados suplantan las huellas digitales de los dispositivos, el uso de estos debe ser validado para que sea confiable.
- Atributos de red y conexión para ayudar a identificar cuándo y desde dónde se conectan los usuarios, y qué tipos de conexiones (web, móvil, VPN, etc.) y encriptación utilizan.
- Información de conducta y biométrica para establecer los patrones de comportamiento de los usuarios —incluidos los patrones de movimiento del mouse y los patrones de cadencia de escritura del teclado— y ayudar a identificar anomalías.
- Análisis del recorrido del usuario para aprender cómo navega un usuario a través de la aplicación e identificar anomalías en su comportamiento.
- Inteligencia del operador móvil para obtener información adicional sobre el riesgo potencial del usuario. Por ejemplo, un usuario con un teléfono prepago de dos días se considera que representa un riesgo mayor que un usuario con una cuenta de tres años de antigüedad. Un teléfono registrado con un operador conocido por ser utilizado por estafadores debido a sus medidas laxas, se considera un riesgo mayor que un teléfono registrado con un operador reconocido.
- Patrones maliciosos, tanto a nivel individual como entre instituciones, para ayudar a detectar intentos de manipular o eludir las medidas de autenticación, así como para identificar la presencia de herramientas de ataque conocidas, como troyanos de acceso remoto (RAT) o malware, están presentes. Esta información puede ayudar a identificar ataques de ingeniería social que pueden dejar una huella difícil de notar en las interacciones digitales.
- Datos de consorcios de usuarios infiltrados y malintencionados de una red mundial para ayudar a detectar a infiltrados conocidos que atacan a otras organizaciones.

Sin esta amplia gama de datos, puede ser mucho más difícil confirmar que un usuario sea realmente confiable.

Establecer confianza a través de los canales digitales

La oportunidad es significativa: cuando puede identificar la actividades potencialmente malintencionadas y confirmar con mayor precisión las actividades legítimas, puede ofrecer más fácilmente la experiencia fluida que exigen los usuarios.

IBM® Trusteer® ayuda a las aseguradoras a establecer una relación digital confiable con los usuarios desde el comienzo de una interacción.
Combina la información integral sobre el comportamiento, las sesiones y los dispositivos de los usuarios con los análisis cognitivos en tiempo real para ayudar a determinar de manera transparente la legitimidad de cada actividad digital y respaldar la autenticación continua basada en el riesgo.

Para lograr esto, la solución Trusteer utiliza un enfoque de "confianza con verificación", que trabaja detrás de escena para descubrir pistas en las actividades digitales que podrían indicar la presencia de infiltrados.

IBM Trusteer puede ayudar a las aseguradoras a establecer confianza en los canales digitales mediante la correlación de valiosos puntos de vista de propietarios con fuentes globales de inteligencia.

Validación de la información del usuario detrás de escena

Con una red global, IBM Trusteer incorpora una amplia gama de datos en su evaluación de riesgo para validar la información del usuario. Estos datos incluyen:

- Inteligencia del operador móvil para evaluar si el número de teléfono proporcionado puede indicar que el usuario no es confiable.
- Inteligencia del dispositivo para identificar si el dispositivo utilizado no es confiable, ya sea que esté comprometido por malware, suplantado por infiltrados o que haya sido usado en el pasado por un infiltrado en otro intento malintencionado.
- Inteligencia de red y sesión para revelar errores de coincidencia en la información de ubicación o señalar metodologías únicas empleadas por ciberdelincuentes, como la ubicación de sus cibertalleres o herramientas únicas y patrones de navegación.
- Biometría del comportamiento que identifica pasivamente el comportamiento del usuario a lo largo de su recorrido para ayudar a separar fluidamente a los verdaderos usuarios de los infiltrados. En el caso de los nuevos clientes, la biometría del comportamiento puede detectar ataques BOT malintencionados o patrones de uso conocidos de infiltrados que están dirigidos al robo de identidad. En el caso de los clientes existentes, la biometría del comportamiento puede aprender los comportamientos de uso de los clientes para poder validar de forma continua y transparente a los usuarios, a medida que estos acceden al sitio para verificar la información de las pólizas, gestionar reclamos o solicitar cambios en las cuentas.
- Inteligencia patentada que se mantiene en la base de datos global de evidencia de IBM Trusteer. Esta inteligencia incluye información sobre evidencia conocida y previamente identificada sobre infiltrados, como direcciones de correo electrónico, números de teléfono, elementos de dispositivos, bandas de crimen organizado y cuentas fraudulentas, toda reunida en base a información de seguridad de cientos de organizaciones de todo el mundo.

Revelación de patrones que indican intenciones malintencionadas

Los infiltrados a menudo demuestran comportamientos diferentes de los usuarios legítimos. Tales comportamientos son a menudo bastante sutiles, como la forma en que ingresan información en una aplicación o la rapidez con la que completan un formulario. Como resultado, IBM Trusteer también identifica e incorpora patrones maliciosos en su evaluación de riesgo utilizando el aprendizaje automático

para analizar una multitud de elementos de datos de dispositivos, sesiones y patrones de uso. Algunos de los elementos de datos analizados incluyen lo siguiente:

- Información sobre el recorrido de los usuarios, incluido cuánto tiempo pasan estos en una página, cómo se completan los formularios, qué tan rápido escriben los usuarios y cómo se ve el recorrido (si coincide con el comportamiento real del usuario o si la información sensorial de la máquina puede levantar sospechas de que algo no anda bien).
- Vínculos de identidad. ¿Se están utilizando los datos para solicitar una nueva póliza o abrir una nueva cuenta utilizada en una aplicación diferente o en otra institución anteriormente?
- Información sobre la actividad de cuentas nuevas. ¿Hay alguna actividad asociada con patrones malintencionados que ocurra después de la creación de una cuenta que pueda indicar que esta fue creada por infiltrados?

Aprovechamiento de la inteligencia entre instituciones

Los infiltrados a menudo usan las mismas tácticas, o los mismos elementos de identidad robados o sintéticos, en diferentes organizaciones.
Como resultado, las soluciones de IBM Trusteer también analizan patrones malintencionados entre proveedores de todo el mundo que están protegidos por las soluciones de IBM Trusteer. Con dicha inteligencia global entre instituciones, IBM Trusteer puede ayudar a las organizaciones a identificar y detectar si:

- la identidad que solicita la cobertura ya ha intentado abrir una o más cuentas a una velocidad y ritmo similares a patrones malintencionados conocidos por otros proveedores protegidos por las soluciones de IBM Trusteer;
- el dispositivo, o los mismos elementos de identidad, solicita abrir varias cuentas en nombre de diferentes usuarios;
- el mismo número de teléfono, correo electrónico o dirección se utiliza en múltiples aplicaciones para diferentes personas.

Conservar la agilidad con la inteligencia adaptativa

¿Qué tácticas usarán los infiltrados en el futuro? Para ayudar a las aseguradoras a obtener la mayor ventaja en un panorama que cambia constantemente, IBM Trusteer utiliza tanto tecnologías avanzadas como especialistas en seguridad de clase mundial para llevar a cabo un seguimiento diario de los cambios en el panorama de amenazas.

La infraestructura de seguridad de Trusteer incorpora nueva inteligencia de manera continua utilizando lo siguiente:

- Capacidades de aprendizaje automático, incluyendo capas de detección y análisis de fraude cognitivo, para comprender, detectar y predecir el riesgo de intentos malintencionados durante las actividades digitales.
- Inteligencia global de amenazas en tiempo real e información global que se ofrece a través de la nube.
- Patrones emergentes seguidos por IBM X-Force®, uno de los equipos de investigación en seguridad comercial más experimentados del mundo.

Esta ampliación continua de los datos proporciona una nueva dimensión de conocimiento y hace que la plataforma sea realmente versátil. Puede ayudar a las aseguradoras a comprender, detectar y predecir rápidamente el riesgo de intentos maliciosos, protegerse contra la evolución de las tácticas de la ciberdelincuencia, aumentar la precisión de las evaluaciones y reducir los costos operativos, todo ello al tiempo que permite una experiencia fluida para el cliente.

Desarrollo de sus propias políticas con la inteligencia avanzada de IBM Trusteer

Las aseguradoras a menudo deben lidiar con una variedad de requisitos comerciales globales y locales, de acuerdo con los patrones de uso que encuentren y la sensibilidad al riesgo de cada institución.

Como resultado, muchas organizaciones buscan el control sobre los modelos que utilizan al evaluar el riesgo potencial. El administrador de políticas de IBM Trusteer les permite a las organizaciones visualizar y adaptar los modelos, y les proporciona la flexibilidad para aplicar nuevas contramedidas y evaluar rápidamente su efectividad, para que sea posible crear nuevas políticas de cuenta con el fin de abordar los requisitos y regulaciones internos y externos.

El administrador de políticas utiliza el aprendizaje automático para sintetizar el conocimiento de las amenazas y tendencias actuales y emergentes que enfrentan las organizaciones y brinda la capacidad de personalizar nuevas políticas, simular reglas y adaptar modelos de riesgo de manera automática o en función de información e inteligencia específicas, todo sin conocimientos previos ni habilidades avanzadas.

Conclusión

La transformación digital está creando nuevas oportunidades para que las aseguradoras puedan fortalecer su compromiso con los clientes, proveedores y profesionales de seguros existentes, así como atraer nuevos clientes y proveedores a través de productos y servicios innovadores. En la era digital, los consumidores, proveedores y profesionales de seguros esperan tener la capacidad para obtener o cambiar información, reclamos y cobertura bajo demanda.

Como resultado, el éxito de las aseguradoras en los próximos años puede depender tanto de lo fácil que sea para los usuarios usar sus canales digitales como de los productos y servicios digitales que estas ofrecen. Más importante aún, a medida que las firmas de seguros buscan ampliar y diversificar las ofertas, las soluciones como Trusteer pueden darse el lujo de ofrecer habilidades dinámicas para aventurarse en esa nueva etapa.

La complejidad de las aplicaciones o procesos, como los múltiples desafíos de autenticación, pueden conducir a la frustración del usuario, afectando los puntajes de satisfacción y con la posible consecuencia del abandono de la experiencia del canal digital por un canal de mayor costo o la oferta de un competidor. Por el contrario, una experiencia digital fluida puede ayudar a las aseguradoras a construir o restaurar la lealtad a la marca y la reputación en el mercado de servicio al cliente.

Al establecer una relación digital confiable con los usuarios, las aseguradoras pueden permitir que los consumidores legítimos soliciten nuevas pólizas, y que los proveedores y profesionales de seguros legítimos inicien sesión en sus cuentas sin requisitos de autenticación onerosos, al tiempo que les exigen a los usuarios identificados como de alto riesgo que cumplan requisitos de autenticación adicionales.

¿Cómo recibirá a los clientes reales en su canal digital? ¿Cómo mantendrá la confianza digital? ¿Cómo mantendrá alejados a los infiltrados?

La solución IBM Trusteer está diseñada para ayudar a las aseguradoras a consolidar esa relación digital confiable de manera rápida y transparente. Valida la información del usuario de forma pasiva, descubre patrones que pueden indicar intenciones malintencionadas y se basa en la inteligencia recopilada de la red global de organizaciones de servicios financieros para ayudar a su organización a≈establecer si el usuario es un cliente legítimo y no un infiltrado enmascarado.

Para más información

Si desea obtener información adicional acerca de las soluciones de evaluación de riesgos de identidad digital de Trusteer, póngase en contacto con su representante o Business Partner de IBM o visite el siguiente sitio web: ibm.com/security/trusteer

IBM Security
Route 100
Somers, NY 10589

Producido en Estados Unidos de AméricaFebrero de 2018

WGW03353-COES-00