IBM Security

IBM

Acelere el crecimiento y la adopción digital con una perfecta confianza en la identidad

IBM Trusteer ayuda a las organizaciones a establecer perfectamente la confianza en las identidades con el proceso de cambio omnicanal del cliente.

Empecemos.

IBM Security

Contenido

Introducción

Si su empresa es como la mayoría, acelerar el crecimiento y aumentar la adopción de canales digitales son prioridades máximas. Las fuerzas del mercado han hecho de las transformaciones digitales una necesidad para que las compañías cumplan con las expectativas de los clientes, llegar a nuevos mercados y aumentar los ingresos.

Pero lo que muchas empresas han descubierto es que volverse digital es solo la mitad de la batalla. Los consumidores exigen una experiencia *a la perfección* en línea – ya sea que realicen una compra, registren una cuenta, se inscriban en un programa o servicio de fidelización o simplemente actualicen su información de contacto.

Cuando los consumidores necesitan llevar a cabo pasos de autenticación adicional para llevar a cabo una transacción, solicitar servicios o acceder a sus cuentas, el canal digital puede convertirse en una fuente de insatisfacción, en lugar de deleite. Esto puede dar lugar a un aumento de las tasas de abandono, siendo que los usuarios se pueden ir a los sitios de un competidor o canales de mayor costo. Y mayores tasas de abandono pueden llevar a bajar las puntuaciones de promotor neto (NPS) y a la pérdida de oportunidades de ventas.

Desafortunadamente, el anonimato del canal digital permite a individuos con las herramientas adecuadas ocultar su identidad y abusar de los canales digitales.

Imagine lo que significaría que las empresas pudieran confiar en verdaderos clientes: transacciones más fluidas, mayor crecimiento digital e innovación y aumento de la competitividad.

A menudo las empresas luchan para confirmar las identidades de los usuarios cuando no tienen información previa o registros de cliente, cuando la información en que se basan está públicamente disponible, y cuando los ciberdelincuentes explotan nuevas funcionalidades digitales, utilizan las identidades robadas o emplean tácticas a través de múltiples canales.

¿Cómo pueden las organizaciones continua y transparentemente establecer confianza en la identidad a lo largo del proceso de cambio digital para que puedan acoger a clientes nuevos, invitados y existentes, manteniendo al margen a la actividad malintencionada?

Para ofrecer una mejor experiencia sin problemas, las organizaciones deberían considerar evaluaciones de confianza de identidad omnicanal multicapas en tiempo real, que analizan una amplia variedad de inteligencia, incluyendo red, dispositivo, entorno, comportamiento e información global.

¿Conoce a sus clientes digitales?

La plataforma IBM® Trusteer® está diseñada para ayudar a las empresas a generar de forma rápida y transparente confianza con los usuarios anónimos, establecer confianza con los nuevos clientes y mantener una relación de confianza con los clientes existentes a lo largo de todo el ciclo de vida omnicanal digital. Cuenta con garantía de identidad digital continua; una plataforma de nube ágil para aumentar la eficiencia; y un servicio de inteligencia en capas con IA avanzada y capacidades de aprendizaje automático.

Las múltiples facetas del establecimiento de confianza en la identidad a lo largo de los canales

Los actores malintencionados pueden fácilmente enmascarar su verdadera identidad. Ellos pueden usar las identidades robadas para abrir nuevas cuentas o registrarse a un servicio o un programa de miembro especial. Pueden comprar productos con robo de datos de pago. Pueden crear identidades falsas o sintéticas (identidades robadas o que agregan datos falsos a identidades verdaderas) para llevar a cabo el fraude de pago, fraude de nueva cuenta e incluso fraude de primera parte. También pueden suplantar a clientes existentes, poniendo en riesgo las cuentas para comprar productos con información de pagos almacenados o capturar datos personales para futuros fraudes.

Para desenmascarar la actividad malintencionada, las empresas necesitan evaluar la identidad de cada usuario en dos niveles esenciales: cómo se conectan al canal digital y quién se está conectando. Incluso si un dispositivo o una conexión parecen legítimos, puede que el usuario no lo sea.

En cada nivel hay multitudes de puntos de datos a considerar. Mientras más datos sean incorporados en las evaluaciones de riesgo, más eficaces serán las evaluaciones de riesgo. Mientras las evaluaciones de riesgo sean más transparentes para los verdaderos usuarios, las empresas podrán ofrecer de mejor manera la experiencia y la confianza que los consumidores esperan. A final de cuentas, en la era digital, las empresas necesitan ser inteligentes acerca de qué usuarios piden completar medidas de seguridad adicionales para confirmar sus identidades.

Evaluación del riesgo a través de una amplia gama de escenarios

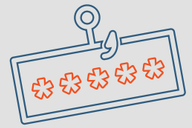
Usuarios

- Clientes invitados
- Nuevas cuentas
- Clientes inscritos
  - Acceso frecuente
- Clientes inscritos
  - acceso raro

Tácticas

- Robo de identidad
- Identidades sintéticas
- Identidades falsas
- Credenciales robadas

Riesgos



- Fraude de pagos
- Abuso de programas de fidelización
- Fraude de primera parte
- Secuestro de cuenta
  - Reclamar puntos
  - uso de datos de pago almacenados
  - cambiar datos de envío
- Fraude de cuenta nueva
- Fugas de datos

Interacciones omnicanal

- Sitio web
- Aplicación móvil
- Llamadas de teléfono celular a call center
- Tienda/sucursal
- Interacciones en vivo de chat/ chatbot

Pistas clave

- Reputación y patrón de e-mail
- Inteligencia de número telefónico celular
- Patrones de comportamiento y ruta de usuario
- Biométrica de comportamiento
- Estado y autenticidad de dispositivo
- Atributos de conexión y red
- Evidencia de spoofing
- Vínculos de identidad
- Datos de consorcio de evidencia maliciosa

Generación de confianza usuarios nuevos, invitados y registrados

La tensión entre seguridad y usabilidad a menudo se siente más intensamente al establecer una relación de confianza con los usuarios anónimos y los nuevos clientes. La solución IBM Trusteer Pinpoint™ Assure está diseñada para ayudar a las empresas a comprender, detectar y predecir el riesgo de intenciones maliciosas para invitados y clientes nuevos. También permite a las compañías realizar supervisión temprana de cuenta para las cuentas nuevas. Funciona de forma transparente para correlacionar ideas patentadas enriquecidas de inteligencia global específica para estos segmentos.

- El análisis de comportamiento y recorrido puede detectar ataques BOT maliciosos o patrones de uso de actividad malintencionada. Esto puede incluir el uso de técnicas y patrones para rellenar formularios digitales, así como los movimientos del mouse, patrones de pulsación y de navegación de sitios web que se relacionan con actividad malintencionada.

- La identificación, asociación, autenticidad y estado de los dispositivos puede identificar si el dispositivo no puede ser confiable, si es víctima de spoofing o está en riesgo por malware o si fue utilizado en el pasado por un actor malicioso en otro intento malicioso. También puede determinar si el dispositivo puede estar asociado con el usuario como dispositivo de confianza.

- La inteligencia de número telefónico puede ayudar a marcar el riesgo incrementado. Por ejemplo, un usuario con un teléfono prepago puede ser considerado un riesgo mayor que el de un usuario con una cuenta de tres años. Un teléfono registrado en una operadora que se sabe que es utilizada por defraudadores debido a sus medidas relajadas, se considera un riesgo mayor que el de un teléfono registrado con una compañía operadora establecida. La información del propietario de la cuenta puede ser conciliada con los detalles de identidad, el registro de información de ubicación, las indicaciones de roaming y estado de línea, y se correlaciona con la inteligencia global y el contexto de usuario y actividad.

- Los vínculos de identidad pueden mostrar si la misma identidad o los atributos de identidad están abriendo nuevas cuentas o realizando transacciones a una velocidad y un ritmo que no coincidan con la actividad legítima en otras empresas protegidas por IBM Trusteer.

- Los datos de consorcio de evidencia maliciosa provenientes de una red mundial pueden ayudar a revelar las actividades malintencionadas.

Los beneficios de la confianza digital para minoristas

- Aumente las suscripciones a los programas de fidelización a través de una seguridad transparente
- Proteja las cuentas de sus clientes contra los riesgos
- Reduzca el abandono causado por la fricción en las medidas de seguridad
- Proteja el recorrido de pago del usuario final

Sostenimiento de la confianza con los clientes existentes

¿Cómo puede mantener una relación de confianza con los clientes suscritos para que pueda ofrecer una experiencia excepcional al cliente cada vez? IBM Trusteer Pinpoint Detect está diseñado para generar de forma transparente perfiles de usuarios y dispositivos para clientes existentes y continuamente autenticar las identidades online para ayudar a detectar secuestros de cuentas o actividad o inicios de sesión no autorizados. Ofrece una visión completa de la actividad del usuario y la cuenta desde varias perspectivas: vistas de dispositivo, sesión de usuario y omnicanal.

- Identificación, autenticidad, estado y evidencia de spoofing en el dispositivo. La identificación del dispositivo puede ser beneficiosa, pero es susceptible a la suplantación y al malware. Una estrategia más robusta incluye varias capas de seguridad que observen la autenticidad, el estado y la evidencia de spoofing del dispositivo junto con la identificación del dispositivo.
- Los atributos de sesión y de red ayudan a identificar dónde y cuándo se conectan los usuarios, qué tipos de conexiones utilizan y cualquier actividad de sesión sospechosa que pueda aumentar los riesgos.
- Los análisis de comportamiento del usuario, de la biometría del usuario y de la ruta del usuario establecen patrones de usuario para ayudar a identificar anomalías, tales como los movimientos del mouse, patrones de escritura o patrones de navegación de los usuarios atípicos a lo largo de la aplicación.
- La inteligencia de patrones maliciosos ayuda a detectar los intentos de eludir o manipular las medidas de autenticación, así como a detectar cuando las herramientas de ataque conocidas como, por ejemplo, Troyanos de acceso remoto (RAT) o malware, están presentes. Este insight puede ayudar a identificar los ataques de ingeniería social que pueden tener un tamaño muy compacto en las interacciones digitales.
- Los datos de consorcio de actor malicioso provenientes de una red mundial pueden ayudar a detectar actores maliciosos que atacan a otras organizaciones.
- Vista omnicanal y entre canales para ver la actividad del usuario a través de las interacciones en web sites, aplicaciones móviles, llamadas desde teléfono celular al call center, tienda/sucursal, y chat o chatbot en vivo.

IBM Trusteer Platform

- Aseguramiento de identidad digital continua
- Plataforma de nube ágil y escalable
- Servicio de inteligencia en capas con IA avanzada y machine learning

¿Por qué IBM Trusteer?

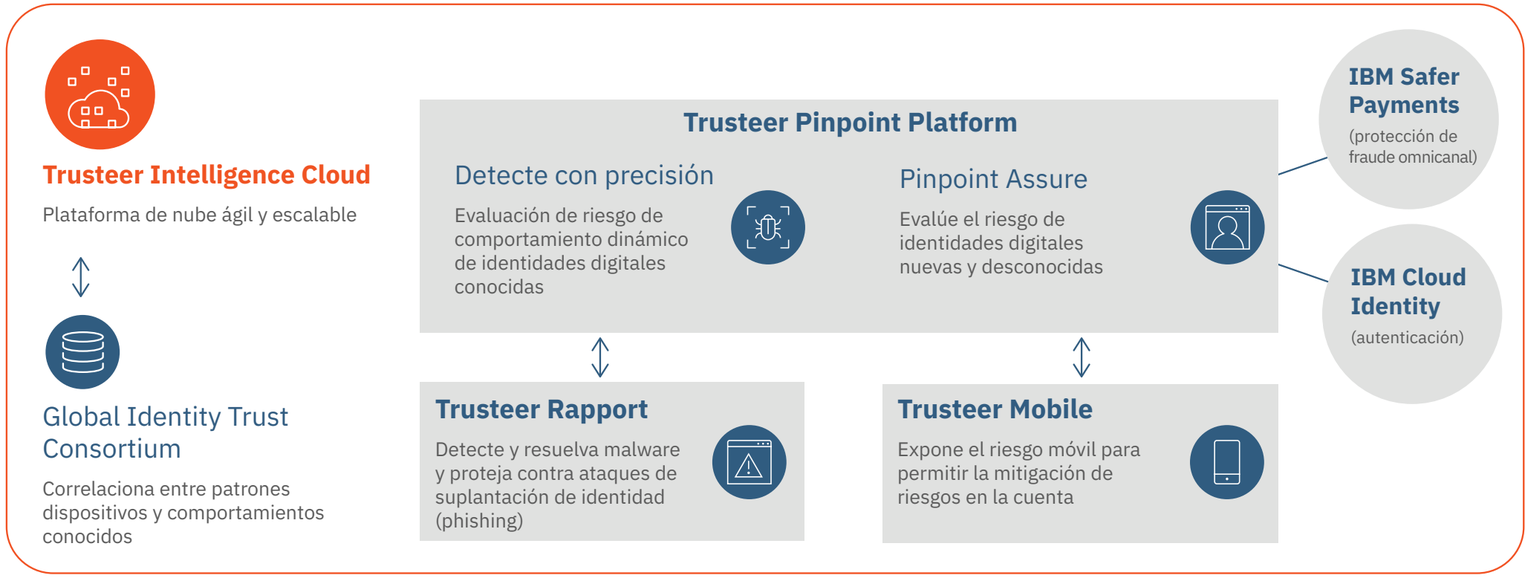
IBM Trusteer ofrece una vista de usuario integral y en múltiples capas, así como un abordaje modular que puede ayudar a las empresas a generar confianza en la identidad de forma transparente con una amplia gama de usuarios para ofrecer una perfecta experiencia de cliente digital.

IBM Trusteer Trusteer se beneficia de su poderoso servicio de inteligencia. Este servicio combina la avanzada tecnología de análisis e IA que analiza miles de millones de sesiones diarias junto con inteligencia humana y experimentados investigadores de amenazas. El consorcio mundial de múltiples organizaciones y el insight de nuevas amenazas se combinaron para identificar patrones emergentes y amenazas cambiantes y adaptar rápidamente las protecciones.

Además, una plataforma de nube ágil y escalable simplifica la implementación y permite evaluaciones de riesgos en tiempo real, con base en la última inteligencia para aumentar la eficiencia operativa y la reducción de costos.

Para obtener más información acerca de la confianza en la identidad transparente de IBM Trusteer, póngase en contacto con su representante de IBM o con un Asociado de Negocios de IBM, o visite el siguiente sitio web: **ibm.com**/security/fraud-protection/trusteer

IBM Trusteer: Descubra la identidad. Genere confianza.



Hable con el especialista

IBM Security

IBM de Colombia S.A.
Cra 53 No. 100 – 25
Bogotá – Colombia

Puede encontrar la página de inicio de IBM en:
ibm.com

Este documento está actualizado conforme a la fecha inicial de la publicación y puede ser modificado por IBM en cualquier momento. No todas las ofertas están disponibles en todos los países en los que opera IBM.

LA INFORMACIÓN PRESENTADA EN ESTE DOCUMENTO SE PROVEE “TAL CUAL” SIN GARANTÍA DE NINGÚN TIPO, NI EXPRESA NI IMPLÍCITA, INCLUSO SIN NINGUNA GARANTIÍA DE COMERCIABILIDAD, CONVENIENCIA PARA UN PROPÓSITO PARTICULAR Y CUALQUIER CONDICIÓN DE NO INFRACCIÓN. Los productos de IBM están garantizados de acuerdo a los términos y las condiciones de los acuerdos bajo los cuales se proporcionaron.

El cliente es responsable por garantizar el cumplimiento de las leyes y las regulaciones correspondientes. IBM no brinda asesoría legal, representa o garantiza que sus servicios o productos garantizarán que el cliente esté en conformidad con cualquier ley o regulación.

Declaración de buenas prácticas de seguridad: la seguridad del sistema de TI incluye la protección de sistemas e información a través de la prevención, detección y respuesta de acceso indebido desde el interior y exterior de su empresa. El acceso incorrecto puede tener como resultado que la información sea alterada, destruida, sustraída o mal utilizada o puede tener como resultado el daño o el mal uso de sus sistemas, incluyendo que sea utilizado en ataques hacia otros. Ningún producto o sistema de TI debería considerarse completamente seguro y ningún único producto, servicio o medida de seguridad puede ser completamente efectivo al prevenir el uso o acceso incorrecto. Los sistemas, productos y servicios de IBM están diseñados para ser parte de un enfoque de seguridad integral y legal, que necesariamente involucrará procedimientos operativos adicionales, y puede requerir otros sistemas, productos o servicios para ser más efectivo. IBM NO GARANTIZA QUE NINGÚN SISTEMA, PRODUCTO O SERVICIO SEA INMUNE DE O HARÁ A SU EMPRESA INMUNE A LA CONDUCTA MALICIOSA O ILEGAL DE CUALQUIER PARTE.

29016929-COES-00