LexisNexis®
RISK SOLUTIONS

LexisNexis® Behavioral Biometrics

Casos de éxito de clientes

El término “Behavioral Biometrics” se utiliza para describir la manera en que un usuario que está en línea interactúa con un dispositivo de escritorio, móvil o portátil mediante su teclado, mouse y/o pantalla táctil. LexisNexis® Behavioral Biometrics fue desarrollado para optimizar el producto LexisNexis® ThreatMetrix® existente con el fin de:

- Agregar otra capa de defensa para la toma de decisiones sobre fraude y riesgo al combinar la manera en que un usuario interactúa con su dispositivo con la inteligencia de identidad digital existente.
- Perfilar de manera óptima el comportamiento de alto riesgo asociado con estafadores, *bots* automatizados, ingeniería social y ataques mediante acceso remoto.
- Desarrollar una vista más clara del comportamiento de usuarios de confianza a lo largo del tiempo, identificando desviaciones de un patrón de comportamiento establecido.
- Identificar perfiles de comportamiento confiables así como de alto riesgo, para hacer una mejor predicción, casi en tiempo real, del comportamiento fraudulento.

Beneficios clave:

Integración estrecha: LexisNexis Behavioral Biometrics está completamente integrada con el portal actual de LexisNexis ThreatMetrix®, optimizando así el alineamiento con capacidades de inteligencia de identidad digital existentes y promoviendo una implementación sencilla.

Enfoque de caja blanca:

- Los datos de Behavioral Biometrics relacionados con las interacciones mediante ratón, teclado o dispositivo móvil están disponibles para ser usados en políticas y reglas.
- Se proveen modelos de aprendizaje automático y calificaciones para categorías de riesgo diferentes, junto con códigos de motivos para exponer la lógica que sustenta las calificaciones. Los atributos de Behavioral Biometrics se pueden utilizar por sí sólos o en combinación con atributos de identidad digital.

Privacidad por diseño: Las teclas alfanuméricas no se registran. Por lo tanto, no se capturan datos de ninguna contraseña o información de identificación personal.

Baja fricción: Se implementa como parte de la carga útil de JavaScript de LexisNexis ThreatMetrix. No hay degradación de desempeño ni impacto sobre latencia cuando se activa Behavioral Biometrics.

Justificación económica de Behavioral Biometrics:

La toma de decisiones confiables sobre riesgo implica cada vez más poner múltiples piezas de inteligencia en capas, de tal forma que se impongan pocas restricciones sobre usuarios legítimos y de confianza. El reto para los negocios digitales es que los estafadores a menudo imitan el comportamiento de usuarios buenos, ya sea haciéndose pasar por clientes legítimos, entrenando a *bots* automatizados para que se comporten como seres humanos o persuadiendo a seres humanos a que inicien transacciones en su nombre.

Los datos de Behavioral Biometrics brindan a las organizaciones otra dimensión de inteligencia al capturar el comportamiento de un usuario final en su dispositivo. La combinación de este conocimiento con la inteligencia de identidad digital relacionada con la reputación del dispositivo, la inteligencia de ubicación, los patrones de comportamiento de las transacciones y las amenazas conocidas, ayuda a las empresas a diferenciar mejor entre los usuarios confiables y las amenazas potenciales.

Behavioral Biometrics en acción: Caso de éxito 1

Dos bancos Tier 1 en EMEA observaron resultados inmediatos después de integrar Behavioral Biometrics a las páginas de creación de cuentas nuevas y registro de canales nuevos.

PROBLEMA DE NEGOCIOS

La creación de cuentas nuevas y el registro de canales nuevos representan un punto de riesgo significativo en la travesía del cliente, ya que los estafadores intentan monetizar credenciales robadas o interceptar un proceso de registro bancario móvil o en línea para tener acceso a cuentas de clientes legítimos.

VENTAJA DE BEHAVIORAL BIOMETRICS

Los estafadores obtienen listas de credenciales de identidad robadas o interceptadas, y utilizan estos datos para inscribirse en forma fraudulenta a nuevos productos o servicios. La captura de datos de identidad digital (p.ej., integridad y ubicación de dispositivo), así como la forma en que un usuario ingresa datos a una aplicación, ayudan a diferenciar entre el comportamiento de usuarios genuinos y el aprovechamiento que hacen los estafadores de las identidades robadas.

RESULTADOS

BANCO A:

70 %
tasa de fraude a una regla que ha identificado patrones de comportamiento recurrentes de alto riesgo en campos específicos dentro del proceso de solicitud de tarjetas de crédito.

92 %
de todo el fraude fue bloqueado por esta regla.

BANCO B:

66 %
tasa de fraude en nuevas inscripciones por medio de aplicación móvil que utilizaban patrones particulares de comportamiento de alto riesgo.

75 %
tasa de fraude en la página de restablecimiento de contraseña cuando se utilizaban funciones específicas del teclado.

Behavioral Biometrics en acción: Caso de éxito 2

Organización de servicios financieros de EE.UU. presenta comportamiento de alto riesgo en solicitudes de tarjetas de crédito nuevas.

PROBLEMA DE NEGOCIOS

La detección de intentos de solicitudes fraudulentas de tarjetas de crédito ayuda a esta organización de servicios financieros a reducir pérdidas por fraude y minimizar exigencias operacionales asociadas con la gestión de cargos revertidos de comerciantes.

VENTAJA DE BEHAVIORAL BIOMETRICS

Se encontró que un estafador se comportaba de una manera notablemente diferente a un usuario de confianza al diligenciar un formulario de solicitud. La utilización del ratón, la cadencia del teclado y el tiempo dedicado a llenar campos contribuyeron a identificar solicitudes de alto riesgo antes de que fueran procesadas.

Usando esta inteligencia, el equipo de servicios profesionales de LexisNexis ThreatMetrix creó un modelo de fraude Behavioral Biometrics personalizado mediante la combinación de datos en bruto de Behavioral Biometrics con analíticas de comportamiento de LexisNexis ThreatMetrix.

RESULTADOS

Incremento entre
10 % y 20 %

Este modelo personalizado de fraude ayudó a lograr un incremento de entre **10 % y 20 %** en la detección de fraude, adicional a las capacidades existentes de identidad digital.

O

1/3

Los falsos positivos se redujeron en **una tercera parte.**

Behavioral Biometrics en acción: Caso de éxito 3

Empresa de viajes global diferencia entre reseñas confiables y fraudulentas utilizando atributos de Behavioral Biometrics.

PROBLEMA DE NEGOCIOS

Las reseñas fraudulentas pueden ser un verdadero dolor de cabeza para las empresas de servicios de viajes. Los estafadores escriben y publican reseñas falsas para dar credibilidad a listas de viajes ficticias o conceder beneficios tramposos.

VENTAJA DE BEHAVIORAL BIOMETRICS

Los viajeros legítimos tienden a escribir reseñas generalmente bien pensadas, mientras que los estafadores a menudo producen reseñas falsas en masa, y esporádicamente cambian detalles clave. Esta diferencia en el comportamiento ayudó a la empresa de viajes a identificar qué comportamientos eran los que más indicaban una reseña falsa.

RESULTADOS

4x

El análisis de cadencia ayudó a revelar patrones de comportamiento en reseñas que resultaron con una probabilidad **cuatro veces** mayor de ser fraudulentas.

2x

El análisis de datos de teclado reveló que las reseñas que no habían sido escritas empezando desde cero tenían una probabilidad casi **dos veces** mayor de ser rechazadas.

Behavioral Biometrics en acción: Caso de éxito 4

Bolsa de criptomonedas logra diferenciación confiable entre tráfico humano y no humano.

PROBLEMA DE NEGOCIOS

Una bolsa de criptomonedas se convirtió en blanco clave de ataques de *bots* automatizados que buscaban capturar cuentas de usuarios legítimos para acceder a monedas digitales.

VENTAJA DE BEHAVIORAL BIOMETRICS

Por su misma naturaleza, el tráfico de *bots* tiene a menudo un patrón de interacción uniforme con negocios digitales, con rasgos que se parecen más a los de las máquinas que a los de los humanos. Aislar estos rasgos de comportamiento le dio a la bolsa de criptomonedas una señal confiable de si el usuario que accedía a una cuenta era un humano o un *bot*.

RESULTADOS

El tráfico de *bots* tenía una velocidad de inicio de sesión **más homogénea** para cada interacción.

Los seres humanos exhibieron a lo largo del tiempo **pequeñas variaciones** en la velocidad de inicio de sesión.

Behavioral Biometrics en acción: Caso de éxito 5

Empresa de juegos de azar en línea asegura pagos al detectar comportamiento de alto riesgo casi en tiempo real.

PROBLEMA DE NEGOCIOS

Las empresas de juegos de azar son blancos claves de delincuentes cibernéticos que buscan retirar fondos fraudulentos, lavar dinero y monetizar tarjetas de crédito robadas.

VENTAJA DE BEHAVIORAL BIOMETRICS

El análisis de datos de teclado reveló que los estafadores que poseen tarjetas de crédito robadas exhiben patrones de comportamiento uniformes que son únicos y distintos de la manera en que los consumidores típicos ingresan datos.

RESULTADOS

32 %

tasa de fraude alcanzada por la empresa de juegos de azar para pagos que exhiben un comportamiento asociado a la utilización de datos de tarjetas de crédito robadas.

Características claves de Behavioral Biometrics


Recolección de datos de mouse y teclado.


Recolección de datos de sensor y pantalla táctil.


Un módulo SDK (kit de desarrollo de software) móvil dedicado.


Los atributos incluyen detección de pegado, mouse fuera de página, elementos de página y tiempos de campos.


Calificación general para cada uno de los siguientes aspectos: biometría de comportamiento, estafadores, anomalías, *bots* e ingeniería social, y códigos de motivos asociados.


Detección de anomalías históricas.


Capacidades de agrupamiento de fraude.


Interfaz de usuario intuitiva, a la cual se accede mediante el portal de LexisNexis ThreatMetrix.

Para más información, visite
risk.lexisnexis.com/fraude

LexisNexis®
RISK SOLUTIONS

Acerca de LexisNexis Risk Solutions

LexisNexis® Risk Solutions aprovecha el poder de los datos y la analítica avanzada para entregar conocimiento que ayuda a las empresas y las entidades gubernamentales a reducir el riesgo y mejorar las decisiones para el beneficio de las personas en todo el mundo. Ofrecemos soluciones de información y tecnología para una amplia gama de sectores, entre ellos: seguros, servicios financieros, salud y gobierno. Con sede principal en la ciudad de Atlanta, Georgia, tenemos oficinas en todo el mundo y somos parte de RELX (LSE: REL/NYSE: RELX), un proveedor mundial de herramientas de analítica y toma de decisiones para clientes profesionales y empresariales basadas en información. Para más información, visite www.risk.lexisnexis.com y www.relx.com.

Nuestras soluciones para servicios financieros ayudan a las organizaciones a prevenir el delito financiero, lograr el cumplimiento regulatorio, mitigar el riesgo de negocios, mejorar las eficiencias operativas y aumentar la rentabilidad.

Este documento tiene fines educativos únicamente y no garantiza la funcionalidad o las características de los productos de LexisNexis mencionados. LexisNexis no garantiza que este documento esté completo o libre de errores.