Hoja de producto

FraudNet

Detección eficaz del fraude conservando la experiencia de cliente. ¿Puedes tenerlo todo?

Para detener a un delincuente, hay que pensar como uno de ellos. El concepto de FraudNet parte de esta premisa para poner en jaque al fraude y optimizar y facilitar la experiencia de cliente. FraudNet se adapta para detectar casos sospechosos y tomar decisiones informadas y acertadas. La vinculación entre varios casos permite identificar temáticas comunes. Si tus sistemas de detección del fraude cuestionan, bloquean o deniegan demasiadas transacciones correctas, tus clientes acabarán por sentirse frustrados. Con FraudNet, sabrás la diferencia entre un estafador y un cliente para proteger tu canal online sin interferir en la experiencia de cliente.

Ventajas de FraudNet

Reduce las pérdidas por fraude

Las tasas de detección del fraude son fundamentales para determinar la eficacia de tu proveedor de soluciones antifraude. Podemos encontrar estos parámetros en diversos informes del sector, publicados anualmente. FraudNet te ofrece una solución integral con tasas de detección del fraude superiores a la media del sector, demostrando reducir las tasas de ataque de manera continuada y a largo plazo. Es un bloqueo a los defraudadores, quienes terminan abandonando sus intenciones fraudulentas, buscando objetivos más vulnerables.

Protege la experiencia de cliente

FraudNet reduce las revisiones y los falsos positivos para agilizar el flujo de clientes honrados y aumentar tu volumen de negocio. Al mismo tiempo que intenta atrapar a los defraudadores, permite que los buenos clientes no vean frustrada su experiencia digital. Poner obstáculos a un buen cliente crea desavenencias innecesarias para tu empresa, lo que se puede traducir en una pérdida de ingresos, una mala experiencia de cliente y una posible publicidad negativa. FraudNet cuenta con los índices de falsos positivos más bajos del sector y no requiere comprobaciones de fraude molestas que interrumpen el acceso a tus servicios (y que posiblemente pongan sobre aviso a los defraudadores).

Desvía el fraude a la competencia

Normalmente, los defraudadores van a por el objetivo más fácil y a por las empresas más vulnerables. Todo intento de fraude contra una empresa se mide a través del indicador de intentos de fraude soportados. Muchos de nuestros clientes han visto una reducción de estos indicadores de ataques después de implementar FraudNet, desviando el fraude a la competencia.

Componentes de FraudNet

Inteligencia de los disposiivos

DeviceInsight. Esta tecnología en tiempo real carece de etiquetas y cookies, y permite a las empresas ir un paso por delante de los defraudadores para no entorpecer la experiencia de cliente. La tecnología en tiempo real y la información de los dispositivos se controlan internamente, de modo que se asigna un ID de DeviceInsight a cada caso, sin tener que usar llamadas ni mensajes, ni tener que recurrir a otro proveedor de soluciones antifraude.

La tecnología en tiempo real compila más de 150atributos de cada página, los combina con los encabezados HTTP y, a continuación, genera un código hash de 40 caracteres, todo ello de forma secreta y confidencial. Además de DeviceInsight, los valores patentados de Time-Differential Linking (TDL) proporcionan aún más nivel de detalle e información del dispositivo que se ha usado.

SDK para móviles. Los dispositivos y las aplicaciones móviles son sinónimos de experiencia digital. Los SDK para móviles se han desarrollado para que las aplicaciones nativas proporcionen aún más nivel de detalle en la identificación de los dispositivos. Los investigadores de Experian han probado cientos de dispositivos diferentes para seguir realizando mejoras tanto de dispositivos iOS como Android. Además de probar numerosos dispositivos, el equipo implementa cambios de acuerdo con las últimas actualizaciones de software, por lo general antes de que las nuevas versiones de software estén disponibles.

Clasificación del riesgo

Motor de riesgos. El motor de riesgos en tiempo real de FraudNet tiene un alto grado de configurabilidad, con más de 600 reglas predefinidas. Además de las reglas estándares disponibles para todos los clientes, se pueden crear reglas personalizadas para detectar patrones de fraude específicos, que se producen dentro de sectores concretos. La combinación de datos de contexto, de comportamiento y de los dispositivos permite a FraudNet identificar más fraudes con menos falsos positivos que cualquier otra solución del mercado.

Gestión de modelos. FraudNet ofrece a los administradores una flexibilidad extra para controlar todos sus modelos de reglas desde la interfaz de usuario, sin tener que depender de ningún equipo de soporte. Los administradores pueden añadir, eliminar y modificar una regla o puntuación en cualquier momento. Los cambios realizados en un modelo surten efecto de inmediato.

Políticas de riesgo. Para atajar los riesgos de forma eficaz, la estrategia adoptada debe trabajar en consonancia con la tecnología. Por ese motivo, el equipo de gestión del riesgo de FraudNet colabora directamente con tu equipo para desarrollar estrategias de prevención, optimizar los modelos de riesgo y compartir conocimientos sobre el fraude en todos los niveles. Esta metodología se sirve de nuestra amplia experiencia adaptada a tus necesidades para ofrecerte la estrategia de prevención del fraude más efectiva.

Patrones de comportamiento. Los administradores de FraudNet pueden personalizar umbrales para identificar a los defraudadores que reutilizan datos o acceden a varias cuentas desde el mismo dispositivo. Esta información puede servir para detectar actividad de programas robot, pruebas de tarjetas, cuentas ruinosas y abusos de períodos de prueba gratuitos.

Herramienta de investigación

Case management. Gestión de casos. La herramienta FraudNet proporciona la información que un investigador necesita, en una interfaz gráfica configurable e intuitiva. Los investigadores pueden buscar un caso específico entre un amplio grupo de casos sin revisar y realizar anotaciones, tomar medidas o seguir investigando según resulte necesario. Confirmar un caso como fraudulento puede añadir automáticamente datos clave predefinidos a la lista negativa, para que en el futuro el fraude se detecte de forma automática. Dentro de la propia interfaz, un investigador puede utilizar los vínculos y enriquecimiento de datos que completan un caso añadiendo aún más información.

DataSpider. . Los investigadores pueden indagar en análisis postforenses si buscan fraudes relacionados con un caso confirmado como malicioso. DataSpider se encarga de hacer esta tarea de forma automática y busca de manera continuada casos vinculados, basados en parámetros de nombre, correo electrónico, teléfono, dirección, ID de usuario y número de tarjeta de crédito cifrado en un intervalo basado en el usuario. Cuando la consulta se ejecuta, los resultados se devuelven codificados por color para mostrar los diferentes vínculos de los distintos casos. DataSpider puede localizar patrones de fraude complejos incluso cuando los defraudadores manipulan la información para tratar de evadir la lógica existente.

SketchMatch. Con DataSpider, los casos vinculados se basan en datos introducidos por los usuarios; en cambio, con SketchMatch se utilizan los datos de los dispositivos. Estos datos son difíciles de evadir y cambiar, y los defraudadores no suelen ser conscientes de qué información se está recopilando. A través del análisis de vínculos, un investigador puede buscar casos vinculados basados en atributos del dispositivo y llegar a descubrir circuitos de fraude.

Listas configurables. Aunque FraudNet proporciona listas positivas y negativas básicas para los datos clave, como dirección de correo electrónico, ID de DeviceInsight, dirección y muchos otros parámetros, cada sector tiene sus propias necesidades y patrones de riesgo, que podrían no aplicarse a los otros. Por tanto, se han creado varias listas específicas por sector a fin de ofrecer una capa adicional de defensa.

Funciones analíticas

Informes estándares. . Mediante seis informes estándares listos para usar, se ofrecen todos los parámetros básicos necesarios para evaluar la eficacia de FraudNet y el equipo de riesgo asociado. Cada informe se centra en un aspecto diferente de la gestión del fraude en una organización con riesgo de sufrirlo.

Resumen del sistema. Este informe ofrece una instantánea de cómo está operando el conjunto de la organización, con cifras de pérdidas y ventas totales.

Resumen de revisiones. Este informe muestra los casos que están pendientes de revisión.

Productividad del investigador. . Este informe evalúa el trabajo del investigador, incluida la cantidad de casos revisados y las medidas que se han tomado. Otros parámetros incluyen cuántos investigadores han aprobado revisiones que posteriormente se consideraron fraudulentas.

Tasa de aciertos de las reglas. Este informe permite a los administradores evaluar la eficacia de cada regla del sistema, a partir de un modelo individual. Se proporciona cada código de regla, sus ajustes actuales y una serie de parámetros. Uno de los principales parámetros es el de capacidad, que es una cuantificación numérica de la eficacia.

Informes personalizados. Además de los informes estándares disponibles, con FraudNet también se pueden crear informes personalizados. Estos informes pueden ejecutarse para un trabajo puntual o planificarse como tareas repetitivas, y pueden guardarse o exportarse para su revisión. Prácticamente todos los campos están disponibles en la interfaz de usuario con fines de elaboración de informes.

Respuesta analítica mejorada. Esta función de análisis complementaria recoge datos de casos, de dispositivos y datos de riesgos avanzados que quedan a disposición de los sistemas. En este informe pueden combinarse los datos de las actividades comerciales realizadas online y sin conexión. Dichos datos son almacenados para su posterior análisis, con herramientas internas de inteligencia empresarial. Esta información combinada puede servir para identificar tendencias y ofrecer una imagen de conjunto de todos los clientes.

Enriquecimiento de datos

Enriquecimiento de datos de terceros. FraudNet usa servicios de enriquecimiento de datos para dar a los investigadores un contexto extra con el que poder hacerse una idea más clara de la situación. Obtener información como la dirección IP o el número BIN es una práctica acertada, pero, por separado, ninguno de estos elementos sirve para tomar decisiones concretas. Saber que el BIN indica una cuenta emitida en el extranjero o que la IP está en la misma ciudad que la dirección de facturación, ofrece más contexto y ayuda al investigador a ir encajando las piezas del puzle.

Contexto sobre el comportamiento. . Los defraudadores son oportunistas e intentan completar todas las acciones a su alcance en el menor tiempo posible, siempre que encuentren las puertas abiertas. Además, suelen actuar con los mismos patrones y hábitos para intentar acceder al proceso de una forma rápida sin ser detectados. Los analistas de riesgos trabajan continuamente para identificar las características específicas de las nuevas tendencias de fraude y los comportamientos de los circuitos de fraude para crear reglas nuevas que atrapen a los delincuentes, a la vez que se reducen al mínimo los falsos positivos y las revisiones de los casos en espera.

Hoja de producto

FraudNet

La prevención del fraude efectiva no solo detiene el fraude

Sin duda, tus esfuerzos para prevenir el fraude van dirigidos a detenerlo y a reducir las pérdidas causadas por éste. Sin embargo, un programa efectivo también facilita que los buenos clientes te escojan y se queden contigo. Entonces, ¿cómo lograr ambas cosas? Empieza porconseguir un enfoque equilibrado en prevención del fraude.. Debe aplicarse el nivel adecuado de protección necesario para cada operación.

Nuestro equipo dedicado a la prevención del fraude, con cerca de 300 expertos en todo el mundo, trabaja para conseguir exactamente eso. Estamos orgullosos del hecho de que este último año hayamos ayudado a nuestros clientes a detectar más de 15 billones de fraudes. Esto equivale a más de 3.300 fraudes por segundo. La mayoría de los consumidores no son conscientes de lo que está sucediendo «entre bastidores» para velar por su seguridad mientras hacen cosas cotidianas como, por ejemplo, comprar en Internet o consultar sus cuentas bancarias desde un dispositivo móvil. Esto lo llamamos «libre de complicaciones», y así es como debería ser. Nuestros sistemas se crean utilizando datos, tecnología y análisis para detener a los defraudadores sin poner barreras a los buenos clientes. Ahora, la prevención del fraude contribuye al crecimiento del negocio y a una experiencia de cliente positiva.

Experian
Calle Príncipe de Vergara, 132
28002 Madrid
www.experian.es