Protege tu hogar digital

Un enfoque multinivel para combatir el fraude

El fraude ya no llama a la puerta: ahora fuerza cerraduras y se cuela por cualquier resquicio.

Imagine su organización como una casa. Si solo protege la puerta principal, las ventanas, las entradas laterales e incluso la chimenea se convierten en objetivos prioritarios para que los intrusos accedan.

Para estar plenamente protegido, necesita un sistema de seguridad integral, no solo una cerradura en la puerta principal.

Al igual que en un hogar, las organizaciones deben proteger todos los puntos de acceso para impedir la entrada de los defraudadores, y la mejor manera de lograrlo es mediante una estrategia antifraude por capas.

Cada capa desempeña un papel esencial para proteger su hogar digital

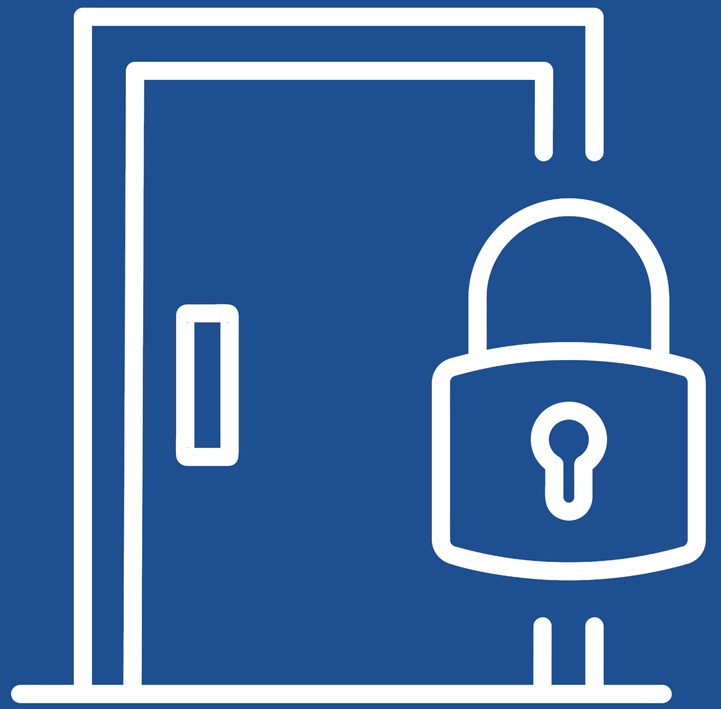
- Análisis del comportamiento
- Verificación de identidad
- Puntuaciones de riesgo de fraude
- Inteligencia de teléfono y correo electrónico
- Señales del dispositivo y de la red
- Verificación reforzada

Análisis del comportamiento, detenga a los intrusos en la puerta de entrada

El análisis del comportamiento es el equivalente digital de una cerradura robusta en la puerta principal: constituye la primera línea de defensa frente a los intrusos.

Al evaluar el comportamiento —como la velocidad de tecleo, los hábitos de navegación y otros factores— se garantiza que solo acceda la persona adecuada. Esto impide accesos no autorizados, protege las interacciones con los clientes y dificulta que los estafadores suplanten a usuarios legítimos.

La analítica de comportamiento ofrece una evaluación de riesgos sólida y discreta desde el primer momento, lo que ayuda a las empresas a actuar como una barrera inteligente y eficaz: mantiene el fraude fuera y permite el acceso únicamente a visitantes legítimos.



El análisis de comportamiento evalúa a la persona, no solo los datos.

Verificación integral de identidad Permita el acceso a quienes corresponda y mantenga fuera a los defraudadores

La verificación de identidad funciona como un sistema de seguridad doméstico: no solo alerta al propietario de posibles intrusos, sino que confirma quién tiene autorización para entrar.

Al confirmar quién intenta acceder, las empresas pueden permitir sin dificultad la entrada a clientes legítimos y, al mismo tiempo, impedir el paso a los estafadores que tratan de colarse con identidades falsas.

Además, al igual que un sistema supervisado que cumple las normas de seguridad, la verificación de identidad ayuda a las empresas a ajustarse a normativas como KYC y AML, creando un entorno fiable y seguro para todas las personas.

La verificación de identidad garantiza que la persona sea quien afirma ser

Las puntuaciones y señales de riesgo de fraude sacan a la luz a los intrusos que acechan en la sombra

Las puntuaciones de riesgo de fraude funcionan como sensores de movimiento en su hogar: analizan de forma continua cualquier actividad inusual y le alertan ante posibles riesgos.

Fraude de primera parte: Imagine a alguien que ya vive en la casa, pero empieza a comportarse de manera extraña, colándose en estancias a las que no debería acceder. El sensor detecta esos cambios sutiles y los marca como sospechosos.

Fraude de terceros: Es el allanamiento más evidente: un desconocido intenta entrar por la fuerza. La alarma se activa de inmediato.

Fraude de identidad sintética: El más difícil de detectar: es como un intruso que se hace pasar por residente. Se mueve con naturalidad para pasar desapercibido, pero los sensores avanzados identifican pequeñas incoherencias que delatan que no pertenece al lugar.

Al igual que los sensores de movimiento añaden capas de protección más allá de la puerta principal, las puntuaciones de riesgo de fraude ofrecen una supervisión continua para detectar amenazas a tiempo, antes de que causen daños.

Inteligencia de teléfono y correo electrónico

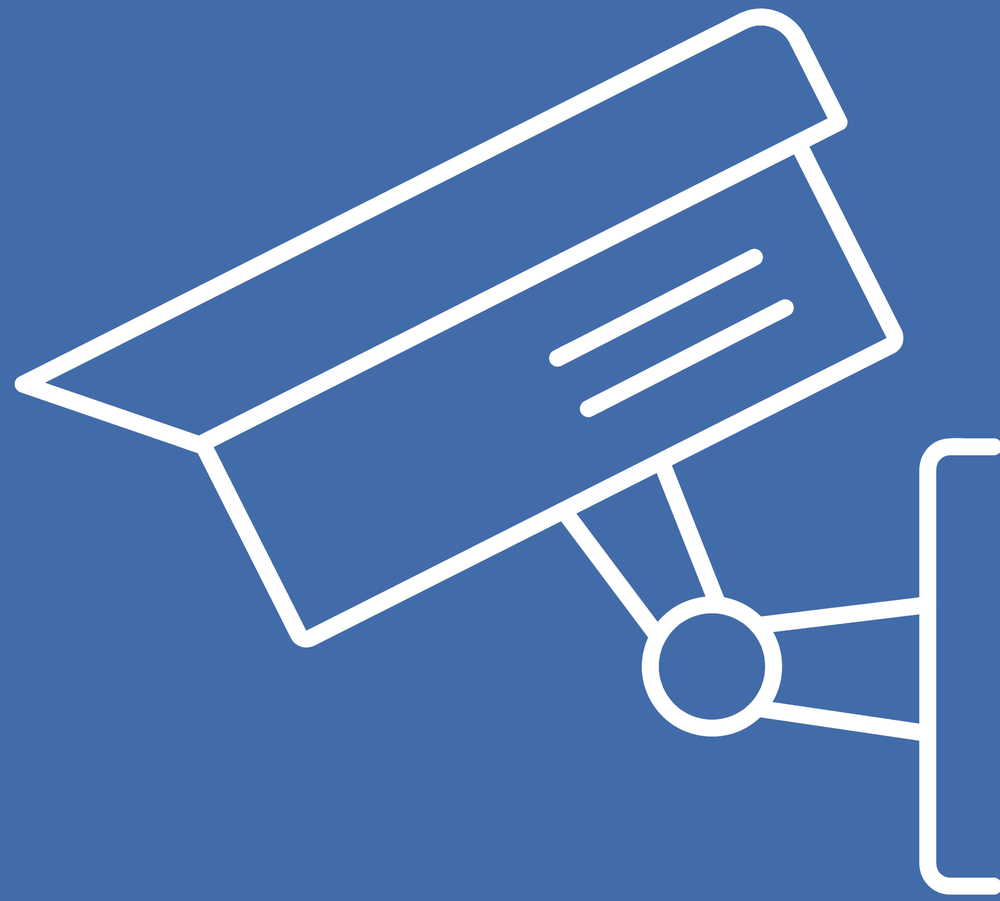
Detecte a los visitantes sospechosos antes de que causen daños

La inteligencia de teléfono y correo electrónico funciona como un timbre con vídeo: no se limita a dejar que alguien llame, sino que le muestra quién está realmente al otro lado.

Al analizar datos como la titularidad del número, el historial del dominio de correo y las señales de riesgo, ofrece a las empresas una visión clara de si el visitante es fiable o supone una posible amenaza.

Al igual que un timbre con vídeo le permite identificar a posibles intrusos antes de abrir la puerta, la inteligencia telefónica y de correo electrónico impide que los defraudadores obtengan acceso ilícito a los servicios, garantizando interacciones más seguras, menores pérdidas por fraude y una mayor confianza de los clientes.

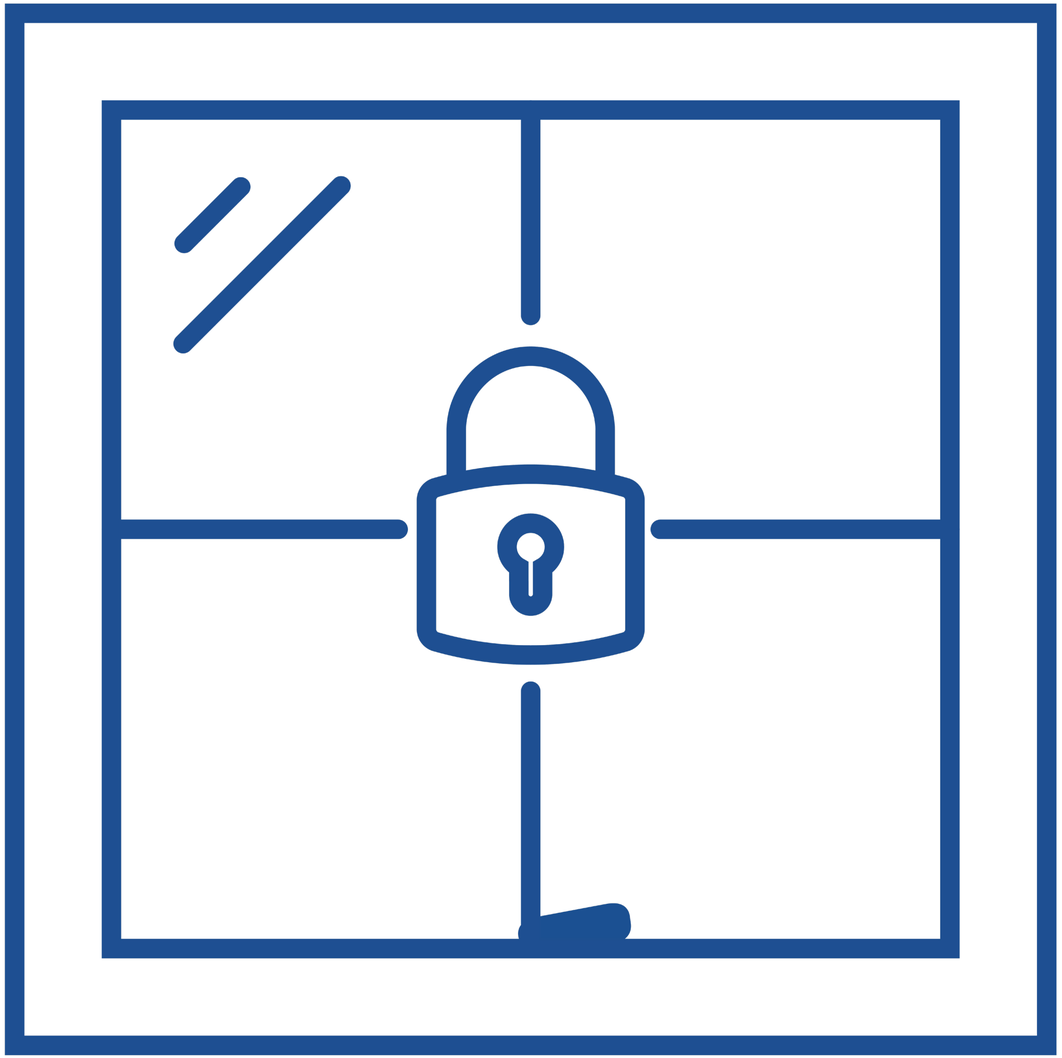
Señales del dispositivo y de la red Detección constante de amenazas digitales



Las señales del dispositivo y de la red son como una cámara de videovigilancia para su entorno digital: no se limitan a comprobar quién ha entrado, sino que siguen observando lo que sucede en toda la casa.

Estas señales supervisan la actividad de forma continua, registrando datos como el tipo de dispositivo, la dirección IP, la geolocalización y los patrones de conexión para detectar cualquier comportamiento inusual.

Del mismo modo que una cámara puede mostrar movimientos sospechosos o rostros desconocidos, el análisis de dispositivos y redes detecta anomalías que las credenciales por sí solas no pueden identificar, lo que ayuda a las empresas a reconocer intentos de fraude en tiempo real y a mantener un perímetro seguro.



Verificación reforzada Su última línea de defensa frente a intrusos

La verificación reforzada es como cerrar con llave las ventanas de su hogar: una precaución adicional que mantiene a los intrusos fuera cuando el riesgo es mayor. Mientras que la cerradura de la puerta principal cubre la seguridad del día a día, las cerraduras de las ventanas aportan una capa adicional de protección para accesos menos evidentes.

Del mismo modo, la verificación reforzada se activa en acciones de alto riesgo mediante herramientas como la autenticación multifactor o la verificación de documentos. Del mismo modo que los cierres de las ventanas impiden que alguien se cuele por un acceso lateral, la verificación reforzada evita que los estafadores aprovechen cualquier vulnerabilidad, fortaleciendo sus defensas cuando más importa.

Un único candado ya no es suficiente Se necesita un enfoque por capas para frenar el fraude en cada punto de acceso

Aunque se lograra superar una barrera, las demás están preparadas para detectar y detener el fraude, creando un marco de seguridad sólido y proactivo que protege a los clientes, las transacciones y la confianza.

Cómo puede ayudar Experian

Le ofrecemos un conjunto completo de capacidades antifraude, integradas en una única plataforma, que aborda todo tipo de riesgos de fraude para ayudar a prevenir pérdidas y captar más clientes de calidad.

- Identifique con mayor precisión a los solicitantes de alto riesgo y aplique el nivel de fricción adecuado.
- Aplique las técnicas de mitigación más apropiadas según el tipo de fraude.
- Reconozca a los usuarios legítimos para que puedan avanzar con rapidez durante el proceso.
- Prevenga, detecte y responda con agilidad para minimizar las pérdidas.

Para obtener más información, póngase en contacto con su representante de ventas de Experian o visite https://www.experian.es/soluciones-empresas/necesidades-empresa/identidad-y-fraude