Fraude de pagos en línea

La inteligencia IP es uno de los cinco métodos que se usa para **detectar y prevenir** el fraude en línea

Accredited by Media Rating Council®

digital element®

Location is Elemental ™

Contenido

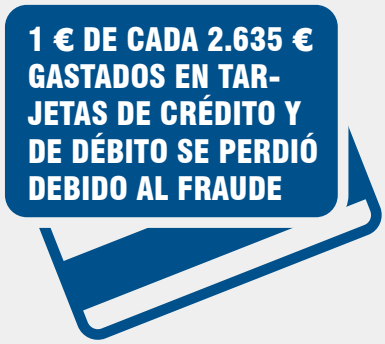
La inteligencia IP: una de las cinco herramientas principales frente al fraude

Según eMarketer, las ventas de comercio electrónico globales se estimaron en 1,8 trillones de euros en 2016, y se espera un crecimiento meteórico de hasta el 75% en 2019. Uno de los inconvenientes de este aumento disparado es el crecimiento de las oportunidades de fraude en línea.
En la Unión Europea, se perdieron 1500 millones de euros debido al fraude. Las pérdidas más cuantiosas fueron en el Reino Unido, con 535 millones de euros, y en Francia, con 429 millones de euros. Unos números significativos, junto con una gestión exhaustiva del proceso de autenticación y la implementación de las herramientas adecuadas, pueden reducir considerablemente el fraude en línea.

El fraude de tarjetas en la zona única de pagos en euros (ZUPE) sigue aumentando, debido a un mayor volumen de fraude en Internet. El tercer informe sobre el fraude de tarjetas, publicado por el Banco Central Europeo (BCE), revela que serán necesarios más esfuerzos para garantizar la seguridad de los pagos con tarjetas a medida que las compras por Internet siguen aumentando.

La implementación de los datos de direcciones IP se encuentra entre las cinco herramientas principales que emplean los comerciantes que usan sistemas de detección automatizados, aunque no todas las soluciones IP se diseñan del mismo modo. Existe un gran abismo entre aquellos que solo se dedican a reempaquetar datos disponibles de manera pública y los proveedores premium, que implementan varias tecnologías para analizar la infraestructura de enrutamiento de IP.

Un nuevo informe del BCE sobre el fraude de tarjetas muestra un aumento del fraude en línea

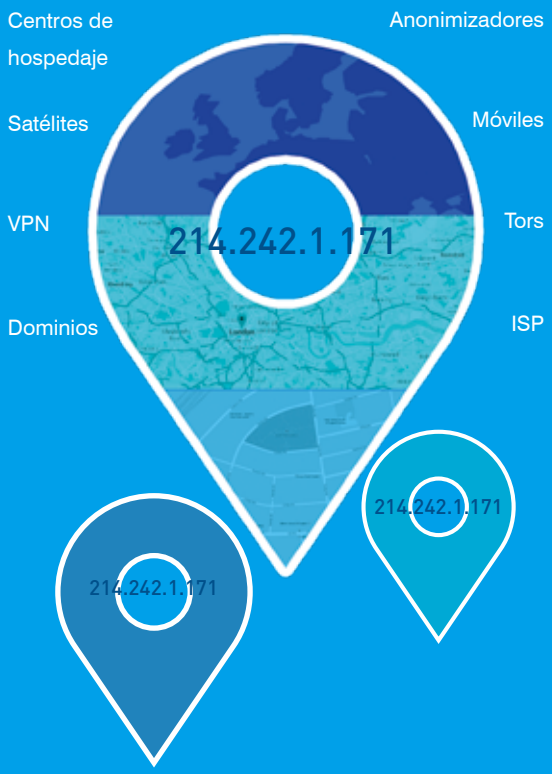


"El fraude de tarjetas en la zona única de pagos en euros (ZUPE) sigue aumentando, debido a un mayor volumen de fraude en Internet. El tercer informe sobre el fraude de tarjetas, publicado por el Banco Central Europeo (BCE), revela que serán necesarios más esfuerzos para garantizar la seguridad de los pagos con tarjetas a medida que las compras por Internet siguen aumentando."

EL SECTOR DEBE SEGUIR MEJORANDO LAS FUNCIONES DE SEGURIDAD, ESPECIALMENTE EN LAS VENTAS POR INTERNET

MÁS TRANSACCIONES POR INTERNET FRAUDULENTAS, EN LÍNEA CON EL FUERTE CRECIMIENTO DE LAS VENTAS POR INTERNET

No todos los proveedores IP funcionan igual



Hay varios proveedores y sistemas que permiten determinar dónde se encuentra una dirección IP y, realizando una pequeña inversión, podemos obtener la ubicación, pero ¿cómo sabemos si es la correcta? Para determinar la ubicación correcta de una dirección IP y descubrir otros datos esenciales de prevención del fraude, como los proxies, se necesita un análisis avanzado de la infraestructura, no basta con solo ir tirando de los registros de Internet o reempaquetando los datos gratuitos disponibles públicamente.

Los datos IP premium de Digital Element, en el nivel más granular, permiten localizar de forma precisa a un usuario en el nivel de sector de código postal o ciudad sin llegar a revelar sus datos personales. La cobertura es global, la precisión es del 99,99 % a nivel de país y los datos se actualizan de manera periódica. Y lo que es más importante, permite determinar cómo se conecta un usuario a Internet y conocer así los datos que los comerciantes necesitan saber para combatir de manera eficiente el fraude, como las VPN, satélites, anonimizadores, tors, móviles, ISP, dominios y centros de hospedaje.

Esto se consigue mediante la combinación del análisis de infraestructuras de enrutamiento IP junto con el conocimiento de ubicaciones anónimas obtenido a partir de una red internacional de socios comerciales.

NetAcuity es una solución integral efectiva que resulta fácil de gestionar internamente y de integrar en los sistemas de los comerciantes. Por el contrario, los datos disponibles públicamente tienen una cobertura global irregular, se actualizan con poca frecuencia y están limitados en cuanto al número de parámetros de datos identificados, además de ser imprecisos de forma intrínseca.

¿Qué tipos de fraude existen?

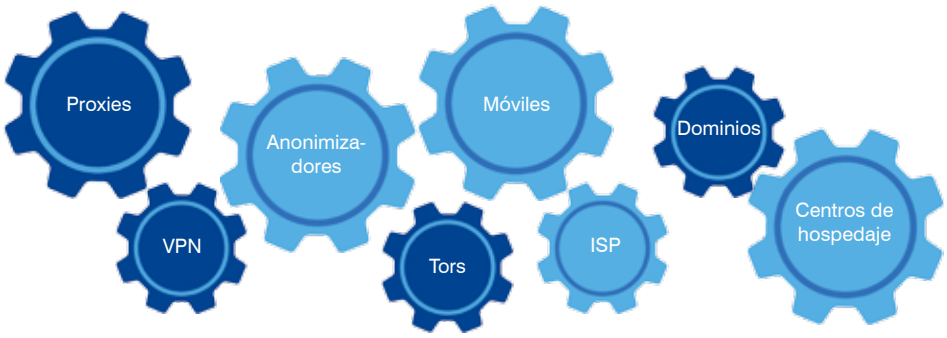
Las principales amenazas para los comerciantes digitales son el fraude limpio, el robo de identidades, el fraude amistoso, el *phishing* (suplantación de identidad) y los botnets. La inteligencia IP NetAcuity de Digital Element ofrece una tecnología que permite exponer el anonimato o descubrir al estafador.

FRAUDE LIMPIO | **ROBO DE IDENTIDAD** | **FRAUDE AMISTOSO** | **SUPLANTACIÓN DE IDENTIDAD** | **BOTNETS**

Invertir en reglas más inteligentes

Se ha demostrado que el diseño de reglas más inteligentes para la detección del fraude y la automatización del proceso permite aumentar las tasas de detección, reducir los falsos positivos y mejorar la experiencia del visitante. La inteligencia IP se puede usar para bloquear automáticamente tráfico sospechoso, solicitar la verificación (por correo electrónico o SMS) o marcar la actividad sospechosa para revisarla en profundidad internamente.

La geografía forma parte del panorama de detección del fraude, por lo que los comerciantes inteligentes van un paso más allá de la ubicación, y usan los parámetros de inteligencia avanzados de NetAcuity para identificar proxies, VPN, anonimizadores, tors, móviles, ISP, dominios y centros de hospedaje. Al ofrecer más datos que solo la ubicación geográfica, la inteligencia IP de NetAcuity puede identificar un mayor volumen de conexiones sospechosas.



¿Qué reglas se deben usar?

Comprobar la dirección IP del país de origen

Una compañía que vende en todo el mundo bloqueará en la mayoría de los casos a países con un alto riesgo de fraude como Nigeria, India, Pakistán o Rusia. Además, si se sabe que un usuario vive en un país específico y accede a una cuenta de otro país, puede levantar sospechas. Un sistema básico "extraído del registro" no puede determinar de forma precisa la ubicación de un usuario. A esto se añade que los datos de IP gratuitos no revelan si un visitante oculta el país desde el que accede a Internet (a través de un proxy o anonimizador), lo que da rienda suelta a posibles actividades fraudulentas.

Ubicaciones de las direcciones de envío y facturación y de la dirección IP

Si las direcciones de envío y facturación y la dirección IP no coinciden, se puede crear una marca roja automatizada para realizar una revisión con más detalle, o solicitar al titular de la cuenta que verifique su identidad a través de correo electrónico o un mensaje.

Nombres de dominio

Se trata de los dominios fraudulentos conocidos y los puntos de conexión a Internet sospechosos como zonas activas Wi-Fi públicas, cibercafés e institutos o universidades.

¿Qué reglas se deben usar?
(continuación)

Proxies
El conocimiento del tipo de proxy con el que un visitante se conecta a Internet, por ejemplo, si es anónimo, transparente, corporativo, público, educativo o AOL puede desencadenar alertas de fraude. Las respuestas al tipo de proxy pueden variar en función del tipo que sea, por ejemplo, un proxy anónimo puede resultar más fraudulento que uno corporativo. Gracias a la identificación de las conexiones que ocultan la ubicación del usuario final o que intentan simular una conexión desde una ciudad o país "aceptable", ahora se pueden crear categorías de manera más sencilla.

Hospedaje
En general, el tráfico del usuario final no se debe observar desde centros de datos u hospedaje, ya que estos tipos de instalaciones están diseñados para que el tráfico pase de un lugar a otro, no para identificar desde dónde se origina. Algunos navegadores en la nube usan estos centros, pero los servicios son irregulares y no están desarrollados con carácter general. Se recomienda contrastar los datos con otro CRM (programa de gestión de relaciones de clientes) antes de confirmar la aceptación de la orden.

Usuario particular, de empresa o ISP
Se pueden añadir otras capas de inteligencia que permiten identificar si una conexión procede de un domicilio o una empresa, además de identificar el proveedor de servicios de Internet (ISP). Los datos se pueden emplear para crear perfiles de la conectividad anterior y evaluar las diferencias o anomalías con el paso del tiempo.

¿Cuándo se deben usar reglas?

Las fases clave de un sistema de autenticación o de pago se producen en el registro, inicio de sesión, compra, depósito de fondos o retirada.

Lo ideal consiste en comprobar de manera continua cada una de las fases del proceso de compra para garantizar que la sesión no se ha pirateado.

Transacciones móviles

Según Gartner, se estima de que los pagos a través del móvil a nivel internacional alcanzarán los 426.000 millones de dólares al final del año. En 2014 se produjo un importante aumento del 31 %.

Cuando se usa un dispositivo móvil para comprar por Internet y se completa la compra, también se crea una conexión IP. Dentro de los usuarios de móviles, es más probable que el 80 % utilice una red Wi-Fi debido a la velocidad, comodidad o coste, y que el 20 % se conecte a través de 3G, 4G o LTE.

Una conexión Wi-Fi es como si fuera un ordenador de sobremesa, en el sentido de que NetAcuity puede determinar con precisión la ubicación Wi-Fi y los tipos de proxy que se usan, por lo que se aplican las mismas reglas que con los dispositivos que no son móviles. Si la conexión se realiza mediante 3G, 4G o LTE, se revelan las características de la red que identifican al proveedor de servicio y su centro de conexión.

Razones convincentes para saber más datos sobre el tráfico

REDUZCA
LA ACTIVIDAD FRAUDULENTA UN
90%

Si conoce desde dónde se conectan los visitantes a un sitio web y cómo lo hacen, es posible que esto revierta en un mayor número de pedidos, menos falsos positivos y un menor volumen de fraude. La clave está en la automatización. Por eso, la inteligencia IP de NetAcuity ofrece una única solución para que las empresas digitales puedan reducir la actividad fraudulenta hasta un 90 %.

NetAcuity es fácil de implementar en un servidor interno (se tarda menos de 20 minutos), varias API suministradas pueden consultar el sistema y el tiempo de respuesta es muy rápido y fiable: inferior a 0,03 milisegundos, lo que permite gestionar hasta 30.000 solicitudes por segundo.

IMPLEMENTE EN UN SERVIDOR
EN MENOS DE 20 MINUTOS

Digital Element es el único proveedor global dedicado de inteligencia IP. Con más de 15 años de experiencia y conocimiento, los equipos especializados de Europa y EE. UU. pueden aconsejarle sobre cómo defenderse del fraude en línea.

Si conoce más datos sobre la procedencia de su cliente y, aún más importante, cómo se conecta, podrá implementar muchas de las mejoras necesarias en los sistemas de comercio.

Algunos datos que facilitamos para proteger a nuestros clientes

País	Tipo de conexión	Zona horaria	ASN
Ciudad/región/estado	Móvil/Wi-Fi	Proxies	Seguridad
Operador de telefonía móvil	Latitud/Longitud	ISP	Particular/Empresa
Código postal	Prefijo telefónico	Dominio	Códigos de actividad industrial
Regiones personalizadas	Nombre de la compañía	Nombre de la organización	Datos demográficos

Curiosidades y datos técnicos de NetAcuity

La plataforma de cliente se integra en todos los sistemas operativos y aplicaciones	Actualizaciones semanales de la base de datos	Inicio y puesta en marcha en tan solo 20 minutos
Baja latencia: 0,03 milisegundos	Capaz de resolver más de 30.000 direcciones IP por segundo	Soporte técnico personalizado disponible para la mayoría de idiomas y plataformas de cliente
Soporte técnico ininterrumpido	Compatibilidad con las plataformas informáticas de 32 y 64 bits, Red Hat Enterprise, Linux 4+, Solaris, 10-Intel, Solaris 8-SPARC, Windows 2003 y 2008 Server	API: C, C++, C#, Perl, Java, PHP, .NET, Ruby y Python

Ejemplos de clientes

VERISIGN · Bankrate, Inc. · JPMorgan Chase & Co. · SONY · intuit · LogRhythm · Western Union · Symantec · intel Security · hulu · SOURCEfire · E*TRADE · Experian · ebay · facebook · DoubleVerify

Póngase en contacto con nosotros para conocer cómo podemos ayudarle a que sus iniciativas en línea sean más competitivas.

Reino Unido | +44 (0)2033 184 702 EE.UU. | +1 678.258.6327
www.digitalelement.com

digital element
Location is Elemental ™