Estudio de caso

BforBank

La tecnología de bases de datos de grafos ayuda a un banco en Internet a desvelar complejos casos de fraude

INDUSTRIA
Servicios financieros

CASO DE USO
Detección y análisis de fraude

OBJETIVO
Reducir el tiempo dedicado a consultar información en sistemas aislados unos de otros y detectar sofisticados esquemas de fraude

RETO
Hay redes y tácticas fraudulentas que a menudo pasan desapercibidas porque se ocultan en diversas capas de falsedad

SOLUCIÓN
Ver las conexiones entre datos para descubrir relaciones ocultas y esquemas de fraude complejos

RESULTADOS
Investigaciones más rápidas con tiempos de respuesta más cortos, y un 20 % más de intentos de fraude evitados. Detección de decenas de casos de fraude que han desenmascarado complejas redes fraudulentas

El banco electrónico francés BforBank tenía que ser más rápido y eficaz a la hora de detectar fraudes y tomar medidas al respecto. Recurrieron a la tecnología de grafos de Neo4j y Linkurious Enterprise para descubrir fraudes complejos mediante la detección de conexiones previamente inadvertidas que abarcaban múltiples silos de datos.

La compañía

BforBank es un banco electrónico fundado en 2009 por el grupo Crédit Agricole. Con más de 180 000 clientes, es una de las principales instituciones financieras del mercado francés de banca en Internet y ofrece servicios tales como cuentas corrientes, de débito y de seguridad, seguros de vida, préstamos hipotecarios y créditos al consumo.

Nuestro socio

Linkurious es desde hace tiempo uno de los socios de soluciones Neo4j, con sede en París. La empresa ayuda a organismos gubernamentales y a compañías de Global 2000 a detectar e investigar con mayor rapidez sofisticadas amenazas. Más de 60 organizaciones de todo el mundo utilizan la plataforma de análisis y visualización de grafos Linkurious Enterprise, una aplicación web distribuida con la que el usuario estándar puede buscar, ver y editar datos guardados en Neo4j. Los equipos de investigación pueden colaborar para utilizar exhaustivas presentaciones de datos y funciones de análisis de grafos, para descubrir conexiones, revelar patrones de interés y encontrar información oculta en datos conectados complejos.

El reto

BforBank tenía grandes dificultades para identificar complejos esquemas fraudulentos en los datos que almacenaba de forma aislada. Los sistemas de gestión de bases de datos de BforBank recopilan diariamente grandes cantidades de datos y el banco tiene diseminados en silos diversos enormes volúmenes de datos, tanto estructurados como no estructurados, desde transacciones y flujo de divisas a documentos de verificación de clientes (KYC, del inglés know your costumer). La supervisión de estos datos es fundamental para reducir los riesgos y las pérdidas financieras. Para realizar investigaciones sobre clientes, transacciones o comportamientos marcados, el equipo de riesgo y cumplimiento del banco utilizaba una solución contra fraude bancario basada en tecnología relacional que hacía muy laborioso, y a veces infructuoso, el proceso de consulta de conexiones en los datos para confirmar la existencia de actividades fraudulentas o descubrir redes de fraude. “Una solicitud podía tardar en resolverse de dos minutos a varias horas cuando había que consultar conexiones a través de múltiples tablas relacionales. Las consultas concernientes a varios campos podían tardar días”, dice Alexandre Dressayre, responsable de cumplimiento normativo de BforBank. Los casos complejos requerían acceso a información dispersa en distintos silos de datos. Algunos tipos de fraude, como el phishing, requerían la intervención del departamento de TI. Cada vez que los investigadores solicitaban recursos técnicos adicionales, se ralentizaba el proceso de

Estudio de caso

"El tiempo de procesamiento para identificar redes de fraude es diez veces menor. En una investigación reciente, bastó media hora para detectar e identificar un grupo de 11 estafadores."

– Alexandre Dressayre, responsable de cumplimiento normativo de BforBank

investigación de fraudes y eso podía dar lugar a mayores pérdidas. El banco necesitaba un modo más eficaz de controlar todos sus datos para reducir riesgos y pérdidas financieras.

La solución

Para mejorar la detección de fraudes y reducir el tiempo de investigación, BforBank recurrió a la tecnología de bases de datos de grafos. Linkurious proporcionó una solución integrada con su software Linkurious Enterprise, que ofrecía visualización y análisis listos para usar sobre la base de datos de grafos de Neo4j. En opinión de Dressayre, era una combinación perfecta. El equipo de riesgos y cumplimiento de BforBank comenzó diseñando un modelo de datos y cargando en Neo4j todos los datos de clientes, transferencias bancarias, actividades de cobro de cheques y direcciones IP. Los datos de grafos estaban disponibles al instante y proporcionaban una interfaz intuitiva para investigar conexiones ocultas de clientes sospechosos. "Gracias a la red de datos disponible, podemos extender las conexiones e intentar averiguar si un estafador está relacionado con otros clientes, por ejemplo, a través de direcciones IP o direcciones postales o de correo electrónico. Esto nos ayuda a detectar redes de fraude o robos de identidad", explica Dressayre. Ahora el equipo de BforBank es capaz de detectar patrones de fraude que anteriormente resultaban demasiado complejos de identificar. "El primer patrón que establecimos fue uno relacionado con el phishing. El sistema notifica casos de clientes con conexiones múltiples y sospechosas", añade Dressayre. A medida que se identifican nuevos tipos de fraude, BforBank puede establecer más alertas adicionales para hacer frente a esas amenazas.

El resultado

Ahora el equipo de riesgos y cumplimiento puede consultar fácilmente conexiones y patrones específicos dentro de los datos, y así descubrir complejos escenarios de fraude que no se habían detectado previamente. Desde la implementación de la tecnología de bases de datos de grafos, BforBank ha notificado un aumento del 20 % en la interceptación de intentos de fraude. Además, el banco ha reducido en gran medida el tiempo requerido para completar las investigaciones, lo que ha contribuido a agilizar decisiones e informes normativos. "El tiempo de procesamiento para identificar las redes de fraude es diez veces menor", dice Dressayre. "En una investigación reciente, bastó media hora para detectar e identificar un grupo de 11 estafadores." Anteriormente, antes de la implementación de Linkurious y Neo4j, un caso de complejidad similar habría tardado varios días en resolverse. Con una visión clara de todas las conexiones de datos, ahora el equipo de riesgos y cumplimiento es capaz de descubrir fraudes y tomar medidas al respecto de forma mucho más rápida y eficiente, preservando la integridad financiera y la reputación del banco.

Neo4j es la plataforma líder en bases de datos de grafos que impulsa la innovación y la ventaja competitiva en empresas como Airbus, Comcast, eBay, NASA, UBS o Walmart. Miles de implementaciones de comunidad y más de 300 clientes utilizan Neo4j para aprovechar datos conectados que revelan interrelaciones entre personas, procesos, ubicaciones y sistemas. Mediante este enfoque basado en las relaciones, las aplicaciones basadas en Neo4j abordan los retos de los datos conectados, como la inteligencia artificial, la detección de fraudes, las recomendaciones en tiempo real y los datos maestros. Más información en Neo4j.com.

¿Tiene preguntas sobre Neo4j?
Contacte con nosotros en todo el mundo:
info@neo4j.com
neo4j.com/contact-us

© 2019 Neo4j, Inc. Todos los derechos reservados.