Étude de cas

BforBank

Une banque en ligne révèle une fraude complexe grâce aux graphes

SECTEUR
Services financiers

CAS D'USAGE
Détection et analyse de la fraude

OBJECTIF
Réduction des délais pour requêter des informations dans des systèmes cloisonnés et détecter des modèles de fraude plus élaborés

DÉFI
Les réseaux et tactiques de fraude restent souvent invisibles car ils s'appuient sur plusieurs niveaux d'indirection

SOLUTION
Visualisation des relations entre données pour mettre à jour des relations dissimulées et des schémas de réseaux de fraude complexes

RÉSULTATS
- Des investigations plus rapides avec des temps de réponses écourtés, et 20 % supplémentaires de tentatives de fraude interceptées
- Détection de plusieurs dizaines de cas frauduleux grâce à la mise à jour de réseaux complexes de fraude

La banque en ligne française BforBank avait besoin de détecter et de riposter aux tentatives de fraude de façon plus rapide et efficace. Elle s'est tournée vers la technologie des graphes de Neo4j et de Linkurious Enterprise pour identifier des relations jusque là invisibles entre de nombreux silos de données et de mettre à jour des fraudes complexes.

L'entreprise

BforBank est une banque en ligne lancée en 2009 par le groupe Crédit Agricole. La banque compte plus de 180 000 clients et fait partie des institutions financières de premier ordre sur le marché français de la banque en ligne. Elle propose des services de comptes chèque, de crédit et de sécurité, des assurances vie, des prêts immobiliers et des crédits à la consommation.

Notre partenaire

Linkurious est un partenaire de longue date de Neo4j, installé à Paris en France. L'entreprise aide les administrations publiques et les entreprises du classement Global 2000 à détecter et à investiguer plus rapidement les menaces complexes. Plus de 60 organisations au monde utilisent sa plateforme intelligente de graphes Linkurious Entreprise.

Cette application web distribuée permet aux utilisateurs non-techniques de faire des recherches dans les données stockées dans Neo4j, de les visualiser et de les modifier. Les équipes sont alors en mesure de collaborer pour exploiter des visualisations enrichies des données et des fonctionnalités d'analyse des graphes afin de mettre à jour les relations, les modèles d'intérêts et les informations utiles dissimulés au cœur de données connectées complexes.

Le défi

BforBank rencontrait une réelle difficulté à identifier des modèles de fraude complexes dans des données cloisonnées. Chaque jour, ses systèmes de gestion de bases de données collectent de grands volumes de données. La banque dispose ainsi de quantités colossales de données structurées et non structurées, distribuées entre différents silos, couvrant les flux de transactions, d'argent, et les documents relatifs au KYC (Know Your Customer, soit l'identification des clients). Or, surveiller ces données est stratégique pour réduire le risque et les pertes financières.

Pour investiguer les clients, transactions et comportements signalés, l'équipe de gestion des risques et de la conformité de la banque utilisait une solution de fraude bancaire à base de technologie relationnelle. Mais requêter des relations au sein de données pour confirmer des activités frauduleuses ou dévoiler des réseaux de fraude s'avérait fastidieux, long et parfois infructueux.

« Une requête pouvait prendre de deux minutes jusqu'à plusieurs heures pour interroger les relations entre les tableaux de nombreuses bases relationnelles. Les requêtes à champs croisés pouvaient prendre plusieurs jours » relate Alexandre Dressayre, responsable de la conformité chez BforBank.

Dans les cas complexes, il fallait accéder à des informations dispersées entre différents silos de données. Certains types de fraude, notamment le phishing, demandaient l'intervention du service informatique.

Étude de cas

« Le temps de traitement pour identifier des réseaux de fraude a été divisé par 10. Dans une investigation récente, un réseau de 11 fraudeurs a été détecté et identifié en une demi-heure. »

– Alexandre Dressayre, Responsable de la conformité, BforBank

À chaque fois que les équipes d'investigation devaient solliciter des ressources techniques supplémentaires, le processus d'investigation était ralenti, provoquant potentiellement des pertes plus importantes. La banque devait trouver un moyen plus efficace de superviser toutes ses données pour réduire les risques et les pertes financières.

La solution

Afin d'améliorer la détection de la fraude et de réduire les délais d'investigation, BforBank s'est tournée vers la technologie des bases de données de graphes. Linkurious proposait une solution combinée dans laquelle le logiciel Linkurious Enterprise apporte une analyse et une visualisation prêtes à l'emploi superposées à la base de données de graphes de Neo4j. Un duo parfait, selon Alexandre Dressayre.

L'équipe de gestion des risques et de la conformité de BforBank a commencé par concevoir un modèle de données en chargeant toutes les données, les demandes de virements, les activités d'encaissement de chèques et les adresses IP des clients dans Neo4j. Le graphe de données a été immédiatement disponible avec une interface intuitive pour explorer les relations cachées des clients suspects.

« Grâce au réseau de données à disposition, nous pouvons étendre les relations et tenter de savoir si un fraudeur est connecté à d'autres clients, par exemple par le biais d'adresses IP, postales ou électroniques. Cela nous aide à détecter les réseaux de fraude ou les vols d'identité frauduleux » indique Alexandre Dressayre.

L'équipe de BforBank est désormais en mesure de détecter des modèles de fraude auparavant trop complexes à identifier.

« Le premier modèle de fraude que nous avons défini concernait le phishing. Le système signale les cas où les clients ont des comportements de connexion multiples et suspects » poursuit Alexandre Dressayre.

De plus, au fur et à mesure que de nouveaux schémas frauduleux sont identifiés, BforBank peut mettre en place des alertes supplémentaires pour repousser ces menaces.

Les résultats

L'équipe de gestion des risques et de la conformité peut maintenant interroger facilement les relations et des modèles spécifiques au sein des données. Elle détecte ainsi des scénarios frauduleux complexes restés invisibles par le passé. Depuis l'implémentation de la technologie des bases de données de graphes, BforBank a constaté intercepter 20 % supplémentaires de tentatives de fraude en cours.

La banque bénéficie également d'une importante réduction des délais pour mener des investigations, ce qui lui permet d'accélérer la prise de décision et la production de rapports réglementaires.

« Le temps de traitement pour identifier des réseaux de fraude a été divisé par 10 » explique Alexandre Dressayre. « Dans une investigation récente, un réseau de 11 fraudeurs a été détecté et identifié en une demi-heure. » Avant l'implémentation de Linkurious et de Neo4j, il aurait fallu plusieurs jours pour venir à bout d'un cas similaire aussi complexe.

Grâce à une vision claire des relations entre toutes ses données, l'équipe de gestion des risques et de la conformité est désormais en mesure de découvrir et d'agir contre la fraude beaucoup plus rapidement et efficacement, préservant ainsi l'intégrité financière et la réputation de la banque.

Neo4j est la plus importante plateforme de bases de données de graphes qui permet à Airbus, Comcast, eBay, la NASA, UBS , Walmart et d'autres d'innover et de rester compétitifs. Des milliers de déploiements par la communauté et plus de 300 clients mettent à profit les données connectées avec Neo4j pour identifier la façon dont les personnes, les processus, les lieux et les systèmes sont interconnectés. Grâce à cette approche par les relations, les applications mises au point en utilisant Neo4j relèvent les défis associés aux données connectées, dont l'intelligence artificielle, la détection de fraude, les recommandations en temps réel et les données de référence.
Pour en savoir plus, consulter neo4j.com.

Des questions sur Neo4j ?

Contactez-nous :
info@neo4j.com
neo4j.com/contact-us