neo4j

Uncover Evolving Fraud Patterns With Graph-Powered Solutions

Get ahead of GenAI fraudsters using Neo4j to complement your AWS investments

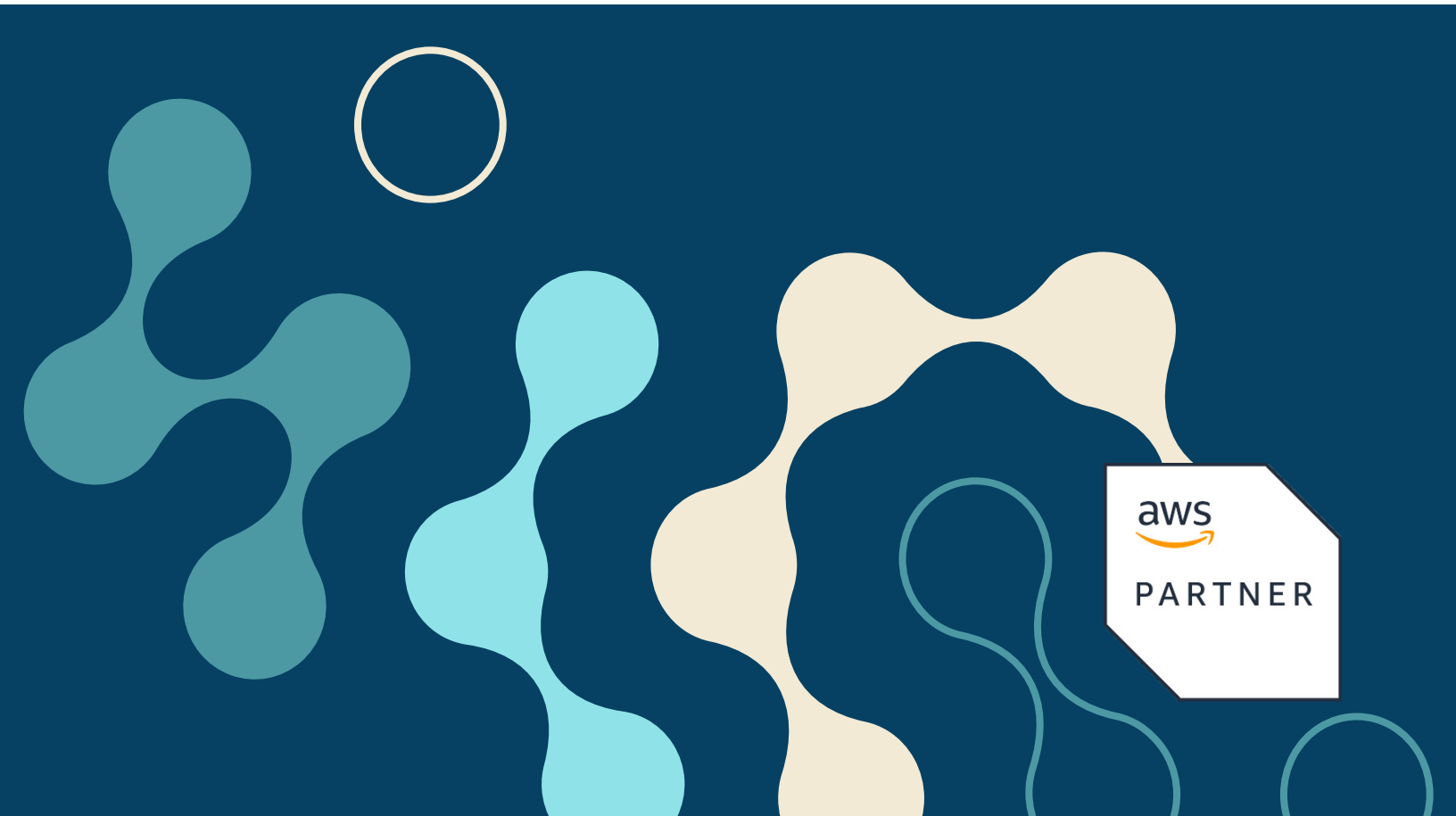
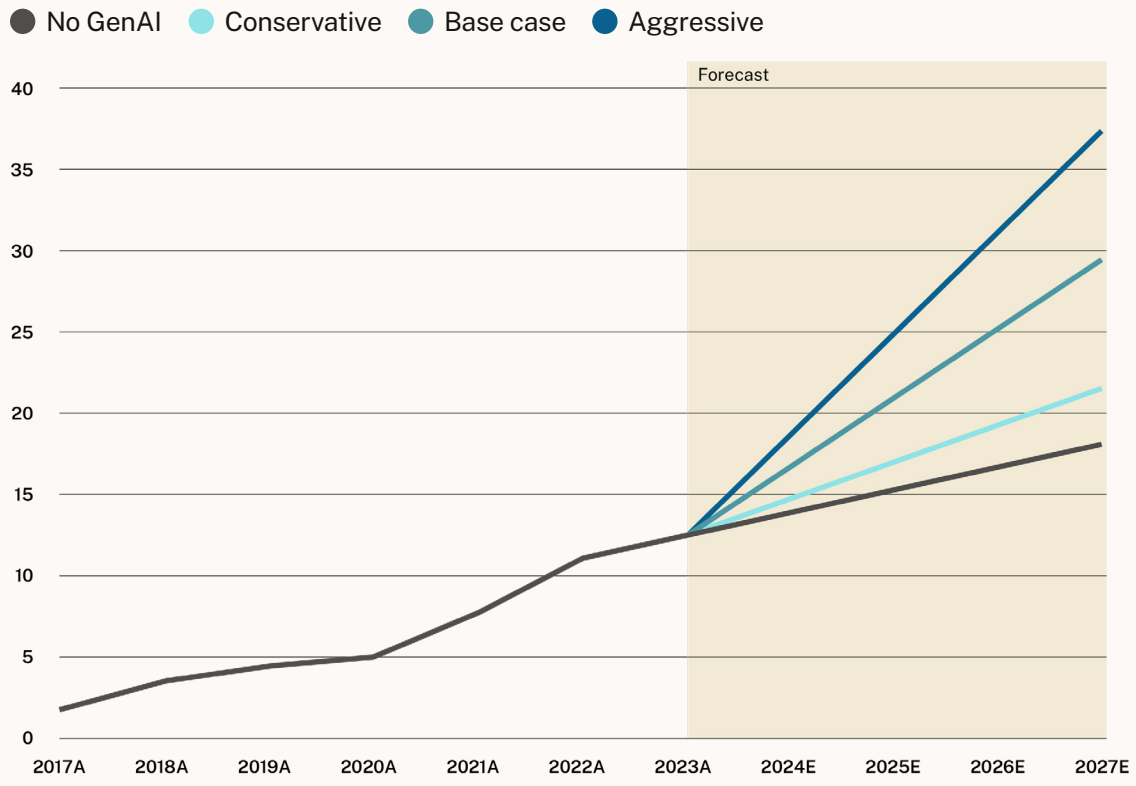


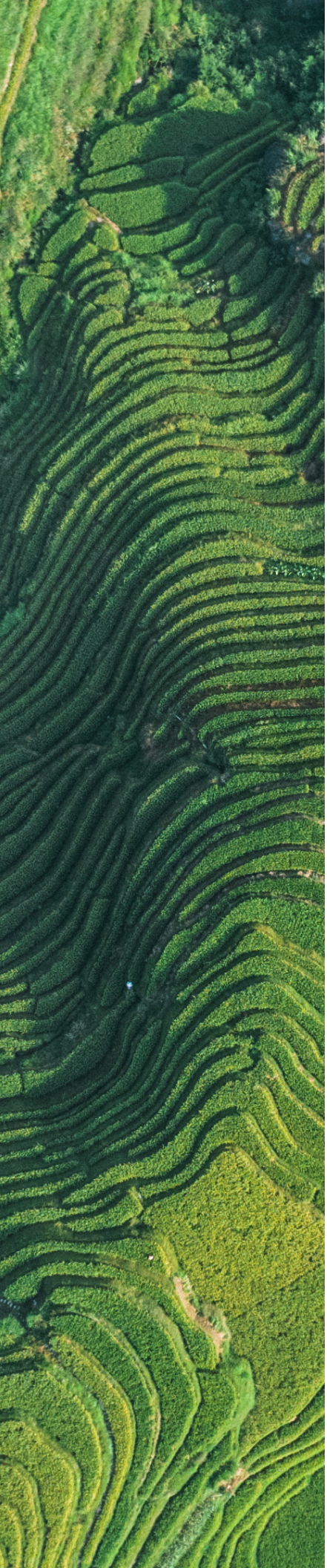
Table of Contents

Generative AI Is Taking Fraud to a Whole New Level — How Will You Keep up?

No one is more excited about the proliferation of GenAI than fraudsters. It's become easy to use and so powerful in its self-learning capabilities that — without the burden of ethical concerns or government regulations — there's not much that can slow it down in the hands of criminals. The Deloitte Center for Financial Services recently published its fraud growth predictions through 2027[1] that account for the use of GenAI. The aggressive model predicts loss up to $40B in one year.

Generative AI is expected to rapidly increase fraud losses in the years ahead.
Fraud losses, actual and expected, 2017 to 2027 ($US billion)





The US Treasury corroborates these trends through its industry report, stating that, “as access to advanced AI tools becomes more widespread, it is likely that, at least initially, cyberthreat actors utilizing emerging AI tools will have the advantage by outpacing and outnumbering their targets,” including financial service and insurance institutions.[2]

The good news is that it’s not all hopeless. According to the Treasury, “many industry experts believe that most cyber risks exposed by AI tools or cyber threats related to AI tools can be managed like other IT systems.” Neo4j offers a flexible, native graph database plus algorithms that you can use to quickly uncover and investigate complex fraud in a way that complements what you’re doing today and helps you get more from your AWS investments.

1. “Generative AI is expected to magnify the risk of deepfakes and other fraud in banking,” Deloitte Insights, May 2024.
2. “Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector,” U.S. Department of the Treasury, March 2024.

Supercharge Your Fraud Detection Solutions With Neo4j Graph Database

Many companies today run a robust fraud detection pipeline that consists of discrete solutions. These work well for known use cases, but what about the new use cases that AI is helping fraudsters develop and exploit? By adding a graph database, you can increase the efficacy of your existing solutions and prepare your team for the upsurge in fraud.

Neo4j Graph Database offers you a deep and intuitive understanding of relationships between entities in your data, which makes it much easier to identify new types of fraud patterns, improve your scoring models, and help ensure your business and customers stay safe.

Building with Neo4j and AWS empowers your team to:

- Enhance your fraud detection solutions with the power of graph
- Improve your outcomes using three key graph design patterns
- Start fast through integrations with existing AWS solutions

Find fraud patterns

1000x faster

than relational databases

Enhance Your Fraud Detection Solutions With the Power of Graph

By its nature, a graph database offers extreme flexibility that traditional relational databases can't match. This makes data exploration and experimentation fluid and intuitive. Layer in new data sets. Uncover connections between entities. Test theories. Do it all and more in a single session with the ease of graph.

As GenAI becomes prevalent among fraudsters, it's important to be able to scale and adapt to evolving threats without having to replace your current fraud detection solutions. The Cypher query language, unique to Neo4j, not only reduces the amount of coding developers need to do, but it also finds larger fraud patterns without needing to be edited.

When you build fraud detection solutions with Neo4j Graph Database, you can uncover complex fraud patterns your current solutions might need weeks to find (if ever). The intuitive data model makes it easy to explore complex data relationships and the developer-friendly schema allows you to link disparate and disconnected data sets quickly. Best of all, you can feed these insights back into your current scoring models to increase their accuracy.

As fraudsters get smarter, you need a reliable way to find and stop fraud before it starts. Neo4j Graph Database helps you continuously evolve your approach without needing to start over.

Zurich Switzerland saved investigators **5-10 minutes per case, or 50,000 hours each year,** with Neo4j.

Read more

Improve Your Outcomes With 3 Key Graph Design Patterns

With a graph database, you can use dynamic fraud detection techniques to provide more accurate results faster. Graph design patterns are a type of abstract technique that you can apply to solve a specific technical challenge. Neo4j offers guidance on how you can use three specific graph design patterns to help you uncover hard-to-find fraud schemes.

1: Pattern Matching

The pattern-matching graph design pattern can uncover fraudulent behavior by displaying the connections and transactions between thousands of entities. First, you specify the pattern you're seeking in the graph: for example, a sequence of nodes connected by relationships that meet defined conditions for account takeovers, payment card fraud, and identity theft. Then, you use Cypher to express this pattern in a query that finds all matching instances.

2: Pathfinding

Pathfinding is the graph design pattern that involves finding one or more routes from a starting point to a destination point. It is used to identify patterns connecting two entities. When you're working with huge data sets for fraud detection, the pathfinding design pattern can show you hidden bad actors in the middle and reveal indirect relationships between entities. It can also predict the likelihood of a future connection between two nodes based on the existing network structure and identify potential fraudulent connections before they fully materialize.

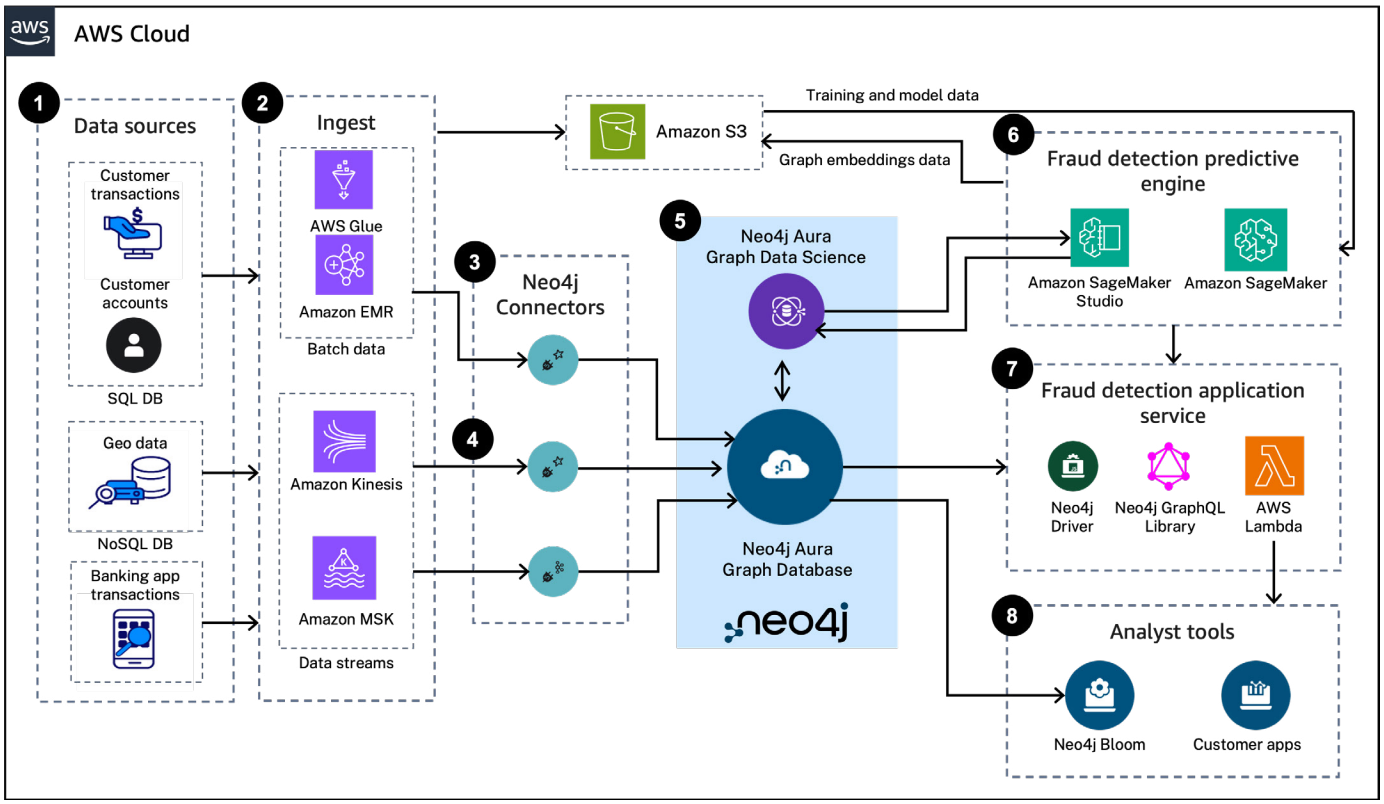
3: Machine Learning

As a graph design pattern, machine learning (ML) helps you discover valuable relationships based on contextual information. This produces signals you can use for feature engineering in the existing fraud detection ML models you're already using as part of your pipeline. Neo4j provides ready-to-use ML algorithms that help you uncover even more sophisticated techniques used by fraudsters like communities and node similarities to hone your feature development.

By using graph design patterns to enhance your existing fraud detection solutions, or build new ones, you strengthen your ability to find and stop threats and reduce false positives.

Start Fast Through Integrations With Existing AWS Solutions

To see how you can get even more value from the AWS resource you're already using today, follow along with the AWS reference architecture. To customize this architecture diagram based on your business needs, download the editable diagram here.



1. Banking transactions, customer accounts, and banking apps clickstream data flow from input data sources.
2. AWS Glue and Amazon EMR ingest, transform, and enrich batch data. Amazon Kinesis and Amazon MSK read real-time data.
3. Connectors for Spark Data Warehouse and Java Database Connectivity load bulk and batch data to Neo4j. You can also use database APIs.

4. Neo4j Kafka Connector or Neo4j Spark Connector streaming APIs ingest clickstream and near real-time transaction and application data from Amazon Kinesis or Amazon MSK to the Neo4j database.

5. The Neo4j Aura Graph Database (GDB) and Neo4j Aura Graph Data Science (GDS) allow you to store, query, analyze, and manage highly connected data. Neo4j Aura is deployed as a SaaS on AWS.

6. Data scientists create novel graph features using embedding algorithms in GDS via Amazon SageMaker Studio notebooks. Embeddings are exported to Amazon SageMaker for improved accuracy. Data scientists can leverage additional graph algorithms, including community detection and similarity in GDS. Data scientists can write graph features back to GDB or relational systems, where they can be easily visualized and analyzed.

7. Scientists can further enhance predictive results by matching patterns and additional information with the graph data. Developers can use Neo4j GraphQL library and drivers to access Neo4j with Java, Node, JavaScript, C#, Python, Go, Ruby, PHP, Erlang, and Perl from AWS Lambda or any application.

8. Neo4j Bloom visualization and customer dashboard tools allow analysts to explore data and present findings.

Scale Fraud Detection With Neo4j in AWS Marketplace

Graph databases are ideal for developing new fraud detection solutions or augmenting existing ones. You can deploy Neo4j Graph Database on AWS using connectors and APIs that work with your existing data ecosystems to help you start using data assets in the cloud and on premises.

Deploying on AWS allows you to scale at the speed and pace you need for your business and find fraud in ever-larger data sets. And by making Neo4j part of your fraud detection pipeline, you can uncover hidden relationships and patterns across billions of data connections deeply, easily, and quickly.

Learn more about how you can enhance your fraud detection solution using Neo4j Graph Database with AWS.

Read: Elevate Fraud Detection With Neo4j on AWS: Uncover Hidden Patterns and Enhance Accuracy

Download: Accelerate Fraud Detection With Graph Databases: How Graph Design Patterns Help You Identify and Investigate Suspicious Activity

Find: Neo4j AuraDB in AWS Marketplace

aws PARTNER