WHY INTELLIGENT APPLICATIONS NEED A GRAPH DATABASE WITH GRANULAR SECURITY

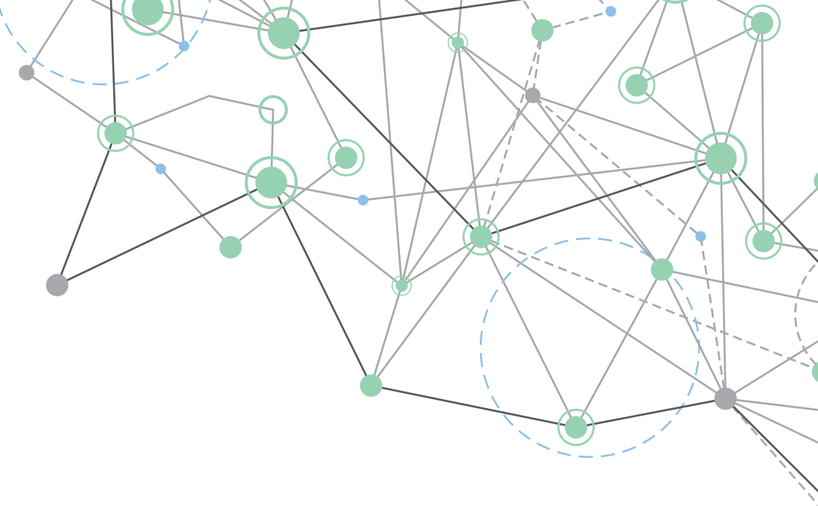
THE CONNECTED SOLUTIONS SERIES

Scalability

Security

Agility

neo4j



Intelligent applications

Intelligent applications come with new requirements. As application development changes, today's databases need to enforce rigorous enterprise security rules while remaining easy to deploy and manage.

Security & Data Privacy

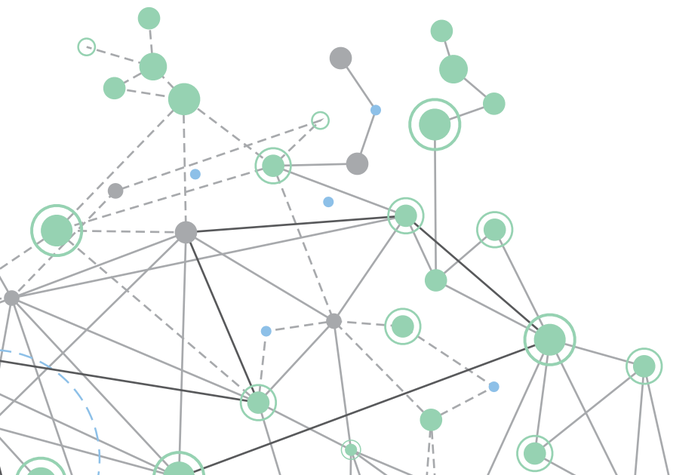
Built in, locked down

Agility

Thrives on change

Unbounded Scale

No limits, no surprises



Enterprise security

Neo4j offers identity and access control using Kerberos and LDAP. Communications with the database take place over Neo4j's internal binary protocol or using HTTPS requests.

TLS Wire Encryption

Users & Roles

LDAP & Active Directory

Property Blacklisting

Security Event Logging

Procedure Access Controls

Intra-Cluster Encryption

Encryption At Rest

Security for graph data

In addition to standard enterprise security features, Neo4j pioneered **schema-based security**, which represents an important advance in the security of graph data.

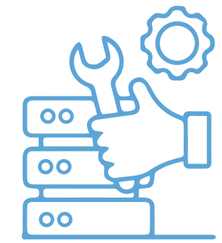
Schema-based security:

- Restricts what data can be seen by different users (role-based access)
- Uses database and schema information to define restrictions
- Applies these restrictions to all database interactions

"The ability to apply fine-grained security on nodes and relationships in a flexible way will have immediate impact across a broad range of use cases."

– Michal Bachman, CEO, GraphAware

Benefits of schema-based security



Governance & Compliance

Govern sensitive data at the schema level, across graph databases

Development Teams

Faster development because security is enforced at the database level

Analysts and Data Scientists

Graph queries, algorithms and AI/ML run only on authorized data

Leadership Team

Reduced risk, increased confidence

Healthcare example

With schema-based security, applications can give doctors a view of a patient's diagnosis and office staff access to schedule appointments, ensuring that only the right users have access to the right data.

Patient Information

Doctor

Office Staff

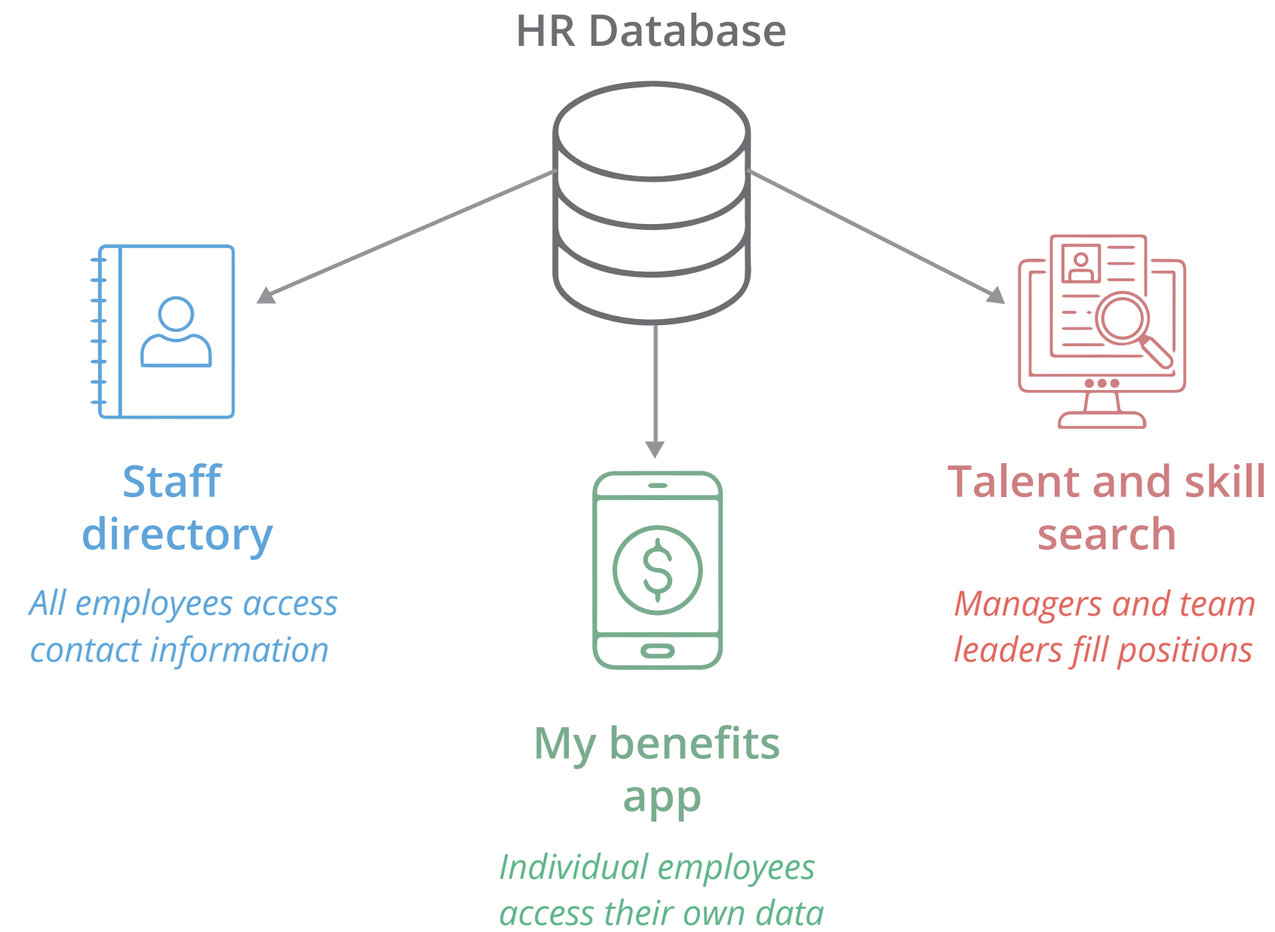
	Doctor	Office Staff
Contact Information	✓	✓
Medical Records	✓	✗
Test Results	✓	✗
Diagnosis	✓	✗

Schema-based security in a medical office

One database, many purposes

With schema-based security, you support more applications using the same graph database.

Think about a human resources database: With the right security rules in place, the same database serves as both an outward-facing staff directory as well as a repository for sensitive HR information.



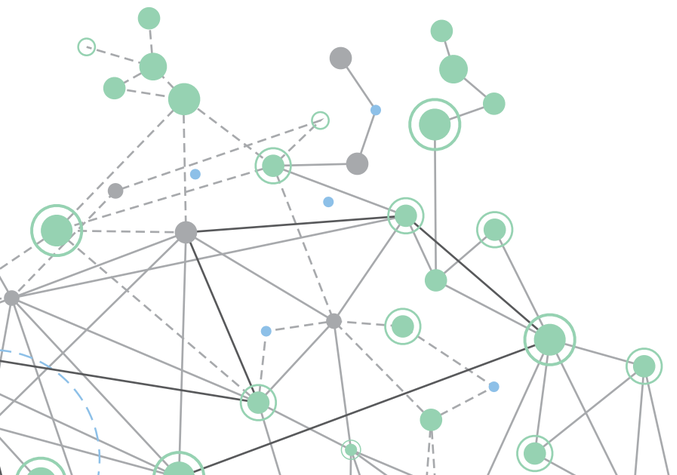
Get started

Robust data security is critical to the future of any business application.

Neo4j offers granular security at the database level to ensure data is protected from the ground up. Role-based access control allows your enterprise teams to use the data they need without exposing the data they don't.

Learn more about schema-based security for graph databases in this white paper on how Neo4j powers tomorrow's connected data solutions.

Neo4j is the world's leading graph database. That's why more than 75% of the Fortune 100 already use Neo4j.



Neo4j is the leader in graph database technology. As the world's most widely deployed graph database, we help global brands – including Comcast, NASA, UBS, and Volvo Cars – to reveal and predict how people, processes and systems are interrelated. Using this relationships-first approach, applications built with Neo4j tackle connected data challenges such as analytics and artificial intelligence, fraud detection, real-time recommendations, and knowledge graphs. Find out more at Neo4j.com.

Questions about Neo4j?

Contact us around the globe:
info@neo4j.com
neo4j.com/contact-us