

LLM

How to Use Graph Database for Cybersecurity

 NebulaGraph 2023-02-01

Have you ever pondered why cyber attackers always appear to be one step ahead of security teams?

It's because their work is much less extensive.

While those who are tasked with defending networks and systems need to identify and block every potential vulnerability, attackers just have to search for a single flaw - no matter how small it is. From this single entry point, they can cause massive damage.

This discrepancy in focus gives attackers greater agility and malleability, allowing them to swiftly take advantage of newly found vulnerabilities.

On the other hand, security teams often find themselves spread thin as they struggle to keep up with an array of constantly evolving cyber threats. They have to make sure they can handle every attack or threat, continually searching all possible sources - which is an overwhelming and extremely time consuming undertaking.

But with the entry of the [graph database](#) era, we can change this and put the attackers behind.

Let's find out.

Graphs for cybersecurity: what does it mean?

It means that for the first time, security teams can get ahead of the cyber attackers.

Many of us might actually be surprised to learn that cyber attackers often view an organization's network from the perspective of a graph. So they mostly concentrate on getting access to just one entry point (node). Using this one entry point, they can construct an attack path to easily penetrate the entire infrastructure.

What about security teams? They have historically relied on lists of alerts from their security systems. Since the lists are simply linear, they don't offer a complete overview.

On the other hand if you were to use the graph approach, it means you'll essentially have a holistic view of the entire infrastructure and you can constantly add to the graph as more items are added to the network. In other words while the attackers are busy looking for an entry point, you have the entire view to yourself. You are now one step ahead as opposed to the traditional list approach where you lag behind.

The concept is really simple: Make use of graph data structures and visualization techniques to represent then analyze it using [graph analytics](#) to unearth cybersecurity issues. This includes data such as network traffic, log files, and malware samples. By representing this data as nodes and edges in a graph, analysts can quickly identify patterns and relationships that may not be immediately obvious in other forms of representation.

Tag

[Features](#)[System-testing](#)[Dev-log](#)[Performance](#)[Use-cases](#)[Community](#)[Deployment](#)[Tools](#)[LLM](#)[Query-language](#)[Graph-computing](#)[Tech-talk](#)[Release-notes](#)[Architecture](#)[News](#)[Source-code](#)[Success-stories](#)[Knowledge-graph](#)[GQL](#)

Top Articles

1 [Benchmarking the Mainstream Open Source Distributed Graph Databases at Meituan: NebulaGraph vs Dgraph vs JanusGraph](#)

2 [Graph Database vs Relational Database: What to Choose?](#)

3 [Difference Between Relational and Non Relational Database](#)

4 [Use cases of graph databases in real-time recommendation](#)

Contents

[Graphs for cybersecurity: what does it mean?](#)

[How to use graphs for cybersecurity \(how it works\)](#)

[Why should your organizations consider switching to graphs for cybersecurity?](#)

[Conclusion](#)

The nodes in the graph represent the data points, such as IP addresses, domains, files, or processes. The edges represent the relationships between the nodes, such as a connection between an IP address and a domain.

How to use graphs for cybersecurity (how it works)

The data from various sources such as network traffic, log files, and malware samples is transformed into a format that can be used to create the nodes and edges of the graph. Once the data is in this format, it can be loaded into a **graph database** as **NebulaGraph**.

Once the data is in the graph, it can be queried, analyzed and visualized. For example, an attack analyst can use graph algorithms to identify patterns and relationships, such as the shortest path between two nodes, which can help them trace the origin of an attack or track the spread of malware. You can also use [graph visualization](#) tools to create interactive diagrams that allow you to explore the data and identify anomalies or potential threats.

Additionally, graph databases can be integrated with other cybersecurity tools such as [intrusion detection](#) systems, network monitoring tools, and threat intelligence platforms. This allows analysts to correlate data from multiple sources, providing them with a more complete picture.

Very briefly, these are the general steps you will undertake when using graphs for cybersecurity:

1. **Data collection:** As mentioned earlier, you'll basically collect data from all the critical points in the infrastructure such as network logs, system events, and security devices. Network logs provide information about the traffic flowing through the network, including IP addresses, ports, and protocols. System events provide information about the activity on a particular system, including user logins, file access, and system updates. Security devices, such as firewalls and intrusion detection systems, provide information about threats and attacks that have been detected on the network.
2. **Data preprocessing:** The goal of data preprocessing is to prepare the collected data for further analysis. This typically involves a series of tasks such as data cleaning, data integration, data transformation, data reduction, and data discretization which is the conversion of continuous data into categorical data.
3. **Graph construction:** The preprocessed data is used to build a graph that can be used to analyze the data and identify patterns that could point to security issues. The process of graph construction typically involves several sub-steps, such as node creation, edge creation, attribute assignment, clustering, and visualization.
4. **Graph analysis:** Involves using graph-based algorithms to analyze the graph built in the previous step and identify patterns, anomalies, and potential threats. There are different types of graph-based algorithms that can be used for graph analysis, such as centrality measures, clustering algorithms, link analysis algorithms, and anomaly detection algorithms.
5. **Threat hunting:** Actively searching for potential threats in the graph, rather than passively waiting for alerts or alarms to be triggered. The process of threat hunting typically involves approaches including hypothesis generation, data exploration, verification, and mitigation.
6. **Remediation:** Can involve anything from implementing a patch or software update to reconfiguring an entire system.
7. **Continuous monitoring and improving:** This could involve adding or removing nodes, changing access control policies, implementing new algorithms, and more.

Why should your organizations consider switching to graphs for cybersecurity?

Graphs offer an all-encompassing, comprehensive look at the network. This perspective has been absent, and as we've observed, this is precisely why security teams are constantly fighting fires.

It's telling that large companies like [Cisco have already started incorporating graphs in their security products](#) - clearly, there's something special about graphs that the major players have uncovered

Fortunately it's not a secret. It's all about these strengths:

Holistic view	The ability to see the interconnectedness of different elements within a network or system. This includes understanding how different nodes and edges relate to one another, and how they may impact the overall security.
Visualization	The ability to represent data in a variety of ways, such as node-link diagrams, heat maps, and matrix plots. These different visualizations can be used to represent different aspects of the data, such as network topology, user activity, and threat detection.
Real-time threat intelligence	Graphs allow for real-time analysis and correlation of data from multiple sources, such as network logs, system events, and threat intelligence feeds. With this, security teams can detect and respond to threats more rapidly.
Prediction	This can involve using machine learning algorithms.
Investigation	While it's not possible to see everything especially when you are dealing with huge data sets, the ability to narrow down to small points within the data and investigate, is a powerful element of a security solution that is powered by graphs. It means security professionals can pick a few nodes and engage them at a higher level.
Compliance	Graph-based security solutions can help organizations comply with industry and government regulations, such as HIPAA, PCI-DSS, and NIST. For example, you'll be able to easily segment and access controls that are required by compliance bodies.
Concentration	This appealing nature of graphs can help analysts stay focused and motivated as they work through large amounts of data. It can also make it easier to communicate their findings to other stakeholders.

All these elements contribute to a cost-effective cybersecurity solution, meaning you can detect and block more threats or attacks at a much more affordable rate than the traditional method of solely relying on lists.

Conclusion

Our brains mostly think best in terms of images, patterns, and relationships. This makes visual representation of data, such as graphs, more intuitive, easier to understand and analyze. Graphs in particular are an effective way to represent complex data and relationships, making it easier to identify patterns, anomalies, and potential threats.

This is why using graphs for cybersecurity is proving disruptive. It's all your security team needs to get ahead of the ever elusive cyber criminals.

How NebulaGraph Works

1. [NebulaGraph Architecture – A Bird's Eye View](#)
2. [Benchmark: NebulaGraph vs Dgraph vs JanusGraph](#)
3. [Comparison: Neo4j vs NebulaGraph vs JanusGraph](#)
4. [Deploy the Graph Database on Kubernetes](#)

LLM



Recommended for you

NebulaGraph Enterprise v5.1

Architecture

NebulaGraph Enterprise v5.1 Embeds Vector Search for AI-Grade Data Fusion

NebulaGraph 2025-05-21

Success-stories

Real-Time Risk Detection at High Concurrency: How EasyCash Secures Growth with

NebulaGraph 2025-05-13

Use-cases

How Airwallex Leverages NebulaGraph for Cross-Border Payment Solutions

NebulaGraph 2025-04-22

Contact us

Contact Enterprise Sales inquiry@vesoft.com

PRODUCTS

NebulaGraph DB

NebulaGraph Cloud

NebulaGraph Studio

NebulaGraph Explorer

NebulaGraph Dashboard

RESOURCES

Docs

Download center

Playground

Blog

COMMUNITY

Forum

START FOR FREE

Live demo

Free Trials

Contact Enterprise Sales

CONTACT US

inquiry@vesoft.com

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our Privacy Policy.

We won't track your information when you visit our site. But in order to comply with your preferences, we'll have to use just one tiny cookie so that you're not asked to make this choice again.

Accept

Decline