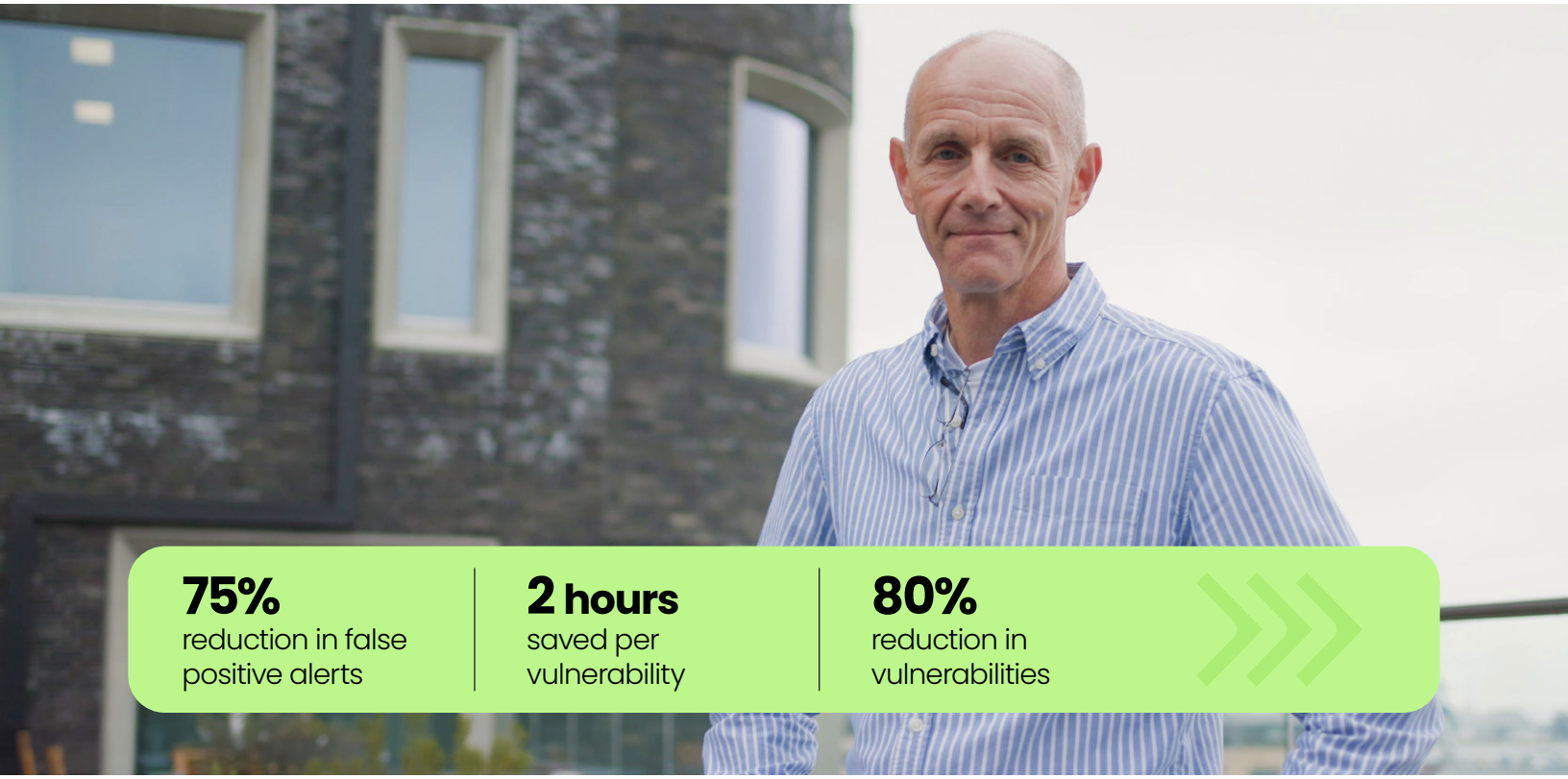
sysdig | CUSTOMER STORY

neo4j

Empowering Engineering to Reduce Risk at Neo4j



Summary

Neo4j, the global leader in graph database technology, needed to maintain customer trust and secure sensitive data across highly regulated environments. Their existing security processes lacked central visibility, overwhelming engineers with false positives and slow remediation cycles. After adopting Sysdig, Neo4j transformed its vulnerability management program with in-use prioritization, automated workflows, and real-time detection. This alignment between security and engineering empowered teams to reduce risk, enable compliance, and accelerate secure innovation..

Key Results

- Security and engineering now work as one team with shared visibility and streamlined workflows
- Junior analysts resolve issues faster with contextual risk paths and real-time prioritization
- Neo4j proactively manages risk instead of reacting to noise or compliance deadlines

Neo4j

Leader in graph databases and analytics for connected data.

HEADQUARTERS

Malmo, Sweden

INDUSTRY

Software Technology

Customer Overview

Neo4j, the graph database and analytics leader, helps organizations find hidden patterns and relationships across billions of data connections deeply, easily, and quickly. Customers leverage the structure of their connected data to reveal new ways of solving their most pressing business problems, including fraud detection, unified profiles, knowledge graphs, supply chain, personalization, Internet of Things, network management, and more – even as their data grows.

Neo4j's full graph stack delivers powerful native graph storage with native vector search capability, data science, advanced analytics, and visualization, with enterprise-grade security controls; scalable architectures; and atomicity, consistency, isolation, and durability (ACID) compliance. Neo4j's dynamic open source community brings together over 250,000 developers, data scientists, and architects across hundreds of Fortune 500 companies, government agencies, and nongovernmental organizations (NGOs).

> "Where cloud security is concerned, you very much need to focus on the crocodile closest to the boat – what's going to bite you and do you real harm? Sysdig helps us be prepared so customers can trust that we're looking after their best interests.
>
> **David Fox,**
> **CISO, Neo4j**

Business Challenges

- Struggled to maintain trust and visibility while protecting sensitive customer data
- Lacked prioritization, leading engineering teams to waste time on low-impact issues
- Faced barriers to achieving SOC 2 compliance with existing processes
- Needed faster access to relevant data to respond quickly to incidents

CHALLENGES

Establishing a Position of Trust

Neo4j provides critical insights to organizations in some of the world's most heavily regulated industries, including NASA and major U.S. banks. A security breach on their platform could have serious consequences. At best, clients would face significant commercial impacts or competitive disadvantages; at worst, they could lose intellectual property or other highly sensitive data.

When David Fox joined Neo4j as Chief Information Security Officer (CISO) in 2022, his first priority was to prevent such a worst-case scenario, starting with securing Neo4j's core offering. "When I first joined, Neo4j's security processes were still maturing, and that journey extended across the organization," Fox said. "Enhancing our security posture quickly became a top priority, as we recognized the importance of building upon our already trusted reputation."

A Matter of Priority

"To me, security has always been about risk management," Fox said. "You can't ever fully secure an organization, so you need to tackle the crocodile closest to the boat. You need a tool that helps you identify your most pressing threats."

For Neo4j, this philosophy highlighted a key area for improvement.

> "We needed one way to look at everything holistically. Not logs here and other things there. We needed everything in one place."
>
> **David Fox,**
> **CISO, Neo4j**

At Neo4j, fixing vulnerabilities is a cross-team sport. "It was our security team's responsibility to identify and communicate the biggest risks," Fox said. "Our engineering team was responsible for implementing fixes. The problem was that our engineering team lacked the visibility to do much on their own."

The disjointed process made vulnerability management a time-consuming and resource-intensive challenge, leaving the company exposed to risk, and underscoring the need for a more cohesive approach.

In addition to a visibility gap and notification overload, Neo4j uncovered significant inefficiencies in their investigation process.

“Gaining a clear security view of our cloud estate was one of the biggest hurdles,” Fox said. “Identifying and prioritizing areas requiring action was both time-consuming and complex. Junior analysts, in particular, struggled with inefficient workflows for understanding and investigating vulnerabilities, which led to extended resolution times.”

SOLUTIONS

Total Visibility

To address their security challenges, Neo4j sought a cloud-native application protection platform (CNAPP) that met several criteria. They needed a solution that was easy to deploy and manage, minimizing the security team’s workload. The platform also had to provide comprehensive, unified coverage across their entire estate. Accuracy, efficiency, and scalability were essential decision factors.

Neo4j ultimately chose to partner with **Sysdig**, deploying its **CNAPP Platform,** which includes **cloud security posture management** (CSPM), a **cloud workload protection platform** (CWPP), and **cloud detection and response** (CDR).

75% reduction in alert noise

Sysdig gave Neo4j a centralized platform to monitor their entire environment, from individual containers to entire clusters, with automated reporting and improved access visibility. Its threat detection module enabled quick identification of activities requiring immediate attention.

“With the deployment of the tool and collaboration with Sysdig experts, we calibrated the system to reduce alert noise by 75%,” Fox said. “This improvement has given us a higher degree of confidence in our monitoring, allowing the security team to focus more effectively on genuine risks.”

Swift Threat Detection

“Most experienced security practitioners regard cybersecurity incidents as not a question of if, but a matter of when,” Fox said. “For Neo4j, our priority was ensuring that we could respond immediately if something bad happened. We wanted to understand exactly what the problem was and how to mitigate it.”

Fox added, “We wanted to be transparent with our customers about any security incidents while maintaining their trust. Achieving that meant knowing what happens in real time, and efficient remediation was nonnegotiable.”

160,000+ vulnerabilities brought to baseline

“At one point, we detected an unusual privilege escalation attempt from a suspicious IP,” said Preeti Gautam, Security Analyst at Neo4j. “Sysdig not only flagged the event but assured us that the individual couldn’t escape their environment. It has also helped us identify issues like orphaned admin accounts.”

Sysdig’s new risk module further streamlines investigations by offering a visual representation of risk paths, enhancing efficiency in analyzing vulnerabilities and alerts. Fox is even exploring how the tool can help upskill junior analysts.

Vulnerability Reporting Reimagined

Neo4j leverages Sysdig to identify in-use vulnerabilities in production workloads, enabling a more focused and efficient approach to vulnerability management. This shift has significantly reduced the volume of reported vulnerabilities by 80% while allowing the team to prioritize and address the highest-risk issues effectively. Analysts now have instant access to detailed information, including affected packages, recommended updates, and remediation steps, all in one place.

“Everything we need is right in front of us,” Gautam said. “We don’t have to switch tools to find fixes or remediation steps. Without Sysdig, it would take me at least two to three hours per vulnerability to manually gather the necessary details.”

In the first six months after deploying Sysdig, Neo4j completely revamped their vulnerability management processes.

“Once the security team identifies a vulnerability, they quickly assess it and forward the details to the engineering team,” said Fredrik Clementson, Senior Director of Engineering at Neo4j. “The engineers then review the vulnerability in Sysdig and implement the required change.”

This streamlined workflow has transformed the collaboration between Neo4j’s security and engineering teams, fostering communication and reducing friction. Together, they’ve successfully reduced over 160,000 vulnerabilities to a benchmark level, giving both teams the confidence that they are now effectively managing risk and maintaining a secure environment.

“One of the biggest benefits of Sysdig has been aligning the security and engineering teams. They speak the same language now,” Clementson said.

Unlocking a New Kind of Collaboration

When Neo4j first deployed Sysdig, it was primarily intended as a tool for their Service Organization Control (SOC) 2 framework. They didn't initially realize its potential as a management tool until they noticed their engineering team proactively addressing low-, medium-, and high-risk vulnerabilities – not just the critical ones flagged by analysts.

> "Engineers aren't anti-security, they're anti-friction. With Sysdig, there is no friction. Our engineers feel empowered to own risk management, which has increased their sense of pride in their work."
>
> **Fredrik Clementson,**
> **Senior Director of Engineering, Neo4j**

Today, Neo4j's engineers handle low- and medium-risk vulnerabilities independently, significantly reducing the workload for the security team. This has not only streamlined operations but also enhanced the quality and security of the company's code.

"Before Sysdig, our teams spoke different languages," Clementson said. "The engineering team didn't always have the evidence to act on security findings. Sysdig was like putting on a new pair of glasses – it gave us the visibility we never had before."

Embracing a Deeper Partnership

While features like in-use vulnerability scanning and the risk module were pivotal in Neo4j's decision to adopt Sysdig, it was the exceptional support and collaboration from the Sysdig team that solidified the partnership. They worked closely with Neo4j to unlock the platform's full potential, transforming it from a tool initially focused on supporting the SOC 2 framework into a comprehensive solution that empowers both the engineering and application security teams to excel in managing vulnerabilities and improving code security.

CONCLUSION

Neo4j's leadership conducts quarterly business reviews with Sysdig to track progress, understand the emerging threat landscape from the **Sysdig Threat Research Team**, and align on long-term goals, thereby cementing an effective partnership.

"Collaborating with other organizations requires mutual understanding and cooperation," Fox said. "Sysdig has excelled in this regard. What we've developed is more than a vendor relationship – it's a true partnership. And that's been one of the biggest benefits of working with Sysdig."

To learn more about Neo4j, visit **neo4j.com**.

neo4j

INDUSTRY

Software Technology

INFRASTRUCTURE

Amazon Web Services, Azure, Google Cloud

ORCHESTRATION

Google Kubernetes Engine

SOLUTION

Sysdig Secure

About Sysdig

Sysdig delivers cloud security the right way with open innovation, agentic AI, and the uncompromising truth of runtime. In a world of black boxes and blind spots, Sysdig helps security and development teams prevent, detect, and respond to threats in the moment.

AI is only as powerful as the signals it receives, and Sysdig Sage™ – the first agentic AI analyst for cloud security – is fueled by the deepest runtime intelligence in the industry. It doesn't just observe. It reasons and acts with the context, speed, and precision that modern teams need to build and defend innovation in real time. Founded by the creators of Falco and Wireshark, Sysdig is trusted by more than 60% of the Fortune 500 and is built for those who refuse to compromise on security.

To learn more about Sysdig, visit sysdig.com.

REQUEST A DEMO →

sysdig

CUSTOMER STORY

CS-NEO4J REV. A 07/25