

# Sophos migrates alert system to Amazon Aurora to improve scalability and enable product innovation

## SOPHOS

### Case study

#### Executive Summary

Sophos, a cyber security company, migrated its alert data to Amazon Aurora from MongoDB databases to improve the scalability of their services and support new capabilities for customers. The engineering team chose Amazon Aurora for its relational database architecture, fully managed services, and scalability. In addition to making the company's whole system more scalable, carving off the alert traffic to run in Amazon Aurora has led to an improved experience for Sophos engineers and end customers.

#### The Challenge

When the company first started, Sophos had one offering and managed their own infrastructure and databases. In five years, they've added dozens of offerings but only made topology changes to the same original server architecture. It's not ideal.

Every month, Sophos receives over 30 million events and alerts from existing customers and must be able to accommodate signals from an additional 5,000 new devices. Since more than just the event workload runs on MongoDB, this exponential increase in data volume over time has resulted in an unfair share of resources that puts pressure on the whole system.

#### The Solution

Migrating event data off the MongoDB databases to the fully managed database service of Amazon Aurora has released the pressure valve on the IT team. They no longer focus on scaling, updating, and managing infrastructure or databases. Instead, they can attend to problems and requests their partners identify to continuously improve their final product and launch new offerings. The relational schema of Amazon Aurora offers engineers the opportunity to provide new service capabilities and insights. And the rest of the business? It finally has the capacity to comfortably scale.

“ Amazon Aurora has become the default choice for any kind of relational data for us because of its ease of use. ”

— John Peterson  
Vice President of Engineering, Sophos

#### About Sophos

As a worldwide leader in next-generation cybersecurity, Sophos protects more than 400,000 organizations of all sizes in more than 150 countries from today's most advanced cyberthreats. Powered by SophosLabs — a global threat intelligence and data science team — Sophos's cloud-native and AI-enhanced solutions secure endpoints (laptops, servers and mobile devices) and networks against evolving cybercriminal tactics and techniques, including automated and active-adversary breaches, ransomware, malware, exploits, data exfiltration, phishing, and more.

The award-winning Sophos Central cloud-based platform integrates Sophos's entire portfolio of best-of-breed products, from the Intercept X endpoint solution to the XG Firewall, into a single system called Synchronized Security. Sophos products are exclusively available through a global channel of more than 53,000 partners and Managed Service Providers (MSPs). Sophos also makes its innovative commercial technologies available to consumers via [Sophos Home](#).

The company is headquartered in Oxford, U.K., and is publicly traded on the London Stock Exchange under the symbol "SOPH." More information is available at [www.sophos.com](http://www.sophos.com).

## Results and Benefits

### Freed up engineers and developers from infrastructure management

Carving off events into a relational database meant that Sophos would have high throughput volumes of data to manage. They didn't want to take on the responsibilities of running a whole new system in addition to their MongoDB deployments. "We knew we didn't want to get into database and infrastructure management again. I want us focused on delivering customer value," says John Peterson, Vice President of Engineering at Sophos. "For us, the decision to move to Amazon Aurora was largely about getting our engineers out of the business of production database administrators."

### Improved the scalability and stability of the entire system

Event data from Sophos customers had been growing at such an alarming rate that the company spent a lot of time thinking about how to scale and manage it. "Finally, we reached a critical mass with managing 10 to 12 million end points across different deployment," explains Peterson. "We were fraying at the seams, and we needed a solution that would support our needs over time." Moving to Amazon Aurora removed scalability and platform stability issues. "No one around here is losing sleep over databases anymore," he added.

### Opened the door for engineers to easily build new capabilities

The migration to Amazon Aurora was, in part, a byproduct of the company-wide move to the microservices approach for development. Not only was the monolithic development process causing scaling issues, but it also delayed application updates and forced engineers to work with data in a sub-optimal environment. "After we decomposed our services, we were able to build more sophisticated features because the alert data was stored and structured in a way that allowed faster innovation," says Peterson. "The move to Amazon Aurora helped us build better features faster and improve productivity for our engineers."

## Learn more

[Amazon Aurora](#) is a MySQL and PostgreSQL-compatible relational database built for the cloud, that combines the performance and availability of traditional enterprise databases with the simplicity and cost-effectiveness of open source databases. Amazon Aurora is up to five times faster than standard MySQL databases and three times faster than standard PostgreSQL databases. It provides the security, availability, and reliability of commercial databases at 1/10th the cost.

---

" The most valuable benefit of moving to Amazon Aurora was being able to count on AWS to manage the database for us. "

— Ravi Gudipati  
Senior Development Manager, Sophos

---