FireEye makes advanced cloud threat detection a reality with Amazon Aurora

Case Study

Executive Summary

The first cloud native API from FireEye, Detection On Demand, integrates threat detection services into a customer's SOC workflow using an API. As part of its larger migration to the cloud, FireEye rearchitected the application to run on Amazon Aurora to take advantage of the database's serverless scalability, improved functionality, and seamless integration with AWS services. Available in AWS Marketplace, Detection On Demand provides an easy way to for AWS customers to add additional layers of security screening to the content and files they store and stream in the cloud.

The Challenge

Millions of requests hit the FireEye Detection On Demand application for approximately two hours every business day when customers first dive into their email to access attachments and hashes. Before moving to AWS, FireEye carried 80% more capacity that they needed during the rest of the day to ensure they could handle peak times. FireEye wanted a solution that matched their cost with demand that could scale without intervention or oversight by their engineers.

The Solution

FireEye rearchitected Detection On Demand to run on Amazon Aurora to take advantage of the improved functionality, scalability, and performance of the database. Using an API, the application integrates into SIEM analytics, SOC workflows, data repositories, and/or web applications to provide submission details including SOC workflows, file, registry, process, and network changes. In its cloud-first form, Detection On Demand makes it easier for AWS customers to identify malicious behavior in files and content stored on AWS services.

> "With Amazon Aurora, we were able to bring Detection On Demand to the market in a matter of months thanks to its serverless architecture and fully managed database services."
>
> — Martin Holste
> CTO, Cloud at FireEye

About FireEye

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber-attacks. FireEye has over 8,500 customers across 103 countries, including more than 50 percent of the Forbes Global 2000.

Detection On Demand marked a significant new accomplishment for FireEye, providing their advanced sandboxing technology to customers as a fully cloud-native service. In order to achieve this milestone, FireEye turned to AWS to run bare metal machines combined with the power of Amazon Aurora.

> "Elsevier leverages FireEye Detection On Demand to protect millions of mission-critical files on AWS."
>
> — Anthony (Glen) Pirrotta
> VP, Cyber Security Engineering & Incident Response at Elsevier, Inc.

Results and Benefits

FireEye Detection On Demand heralds the company's intentional move to a highly scalable microservices environment on Amazon Aurora.

Faster time to market with managed services and consumption-based pricing

In the past, getting a solution to market has been a two to three-year process for FireEye because they were bogged down by budgeting and infrastructure set up. Typically, the process started with developing long-term popularity projections to justify upfront infrastructure investments that would sustain customer demand 3-5 years into the future.

With Amazon Aurora's consumption-based-pricing, the financial request was small compared to what it would have otherwise been, which made the approval process a breeze. Similarly, the managed infrastructure platform of Amazon Aurora allowed engineers to start developing on day one without having to slog through metal and wires. "The beauty of leveraging AWS serverless architecture, is that all those services are managed for us," explained Sai Vashisht, Distinguished Engineer at FireEye. "Furthermore, we can justify increased costs over time better because we'll be able to show direct increase in demand."

Better scalability through serverless technology

FireEye experiences dramatic daily swings in the demand for its services. The first two hours of a business day correspond to a thousand-fold influx of requests from customers as they begin to access email and their files. Building on Amazon Aurora allows FireEye to scale up and down gracefully without needing to carry excess capacity for 22 of every 24 hours.

Reduced time-to-triage through tight integration with AWS ecosystem

The first step to threat remediation is identifying what is failing. AWS microservices architecture allowed FireEye to move away from manual processes, automating the process for isolating failures, making them easily and immediately accessible to engineers in the dev cue. The benefits are game changing for Sai and his team, "We're saving a ton of time using AWS to triage for us, without needing to write a single line of code."

More efficient access to our customers and their data sources

Many FireEye cyber security solutions run on AWS, where the vast majority of their clients already operate. This compatibility allows FireEye to act a clearinghouse for security and become integral part of their customers' workflows. By building Detection On Demand as a 100% native application, FireEye can achieve even greater speed, service, and security synergies through the AWS ecosystem. "Being on Marketplace has been a big goal for us for a long time," explained Martin Holste, CTO, Cloud at FireEye, "and the reliability that Amazon offers, helps us achieve our cloud goals."

> "One of the ways we measure success of our projects is by the number of SREs/Operation personnel needed. A number of projects on Amazon Web Services have required zero."
>
> — Martin Holste
> CTO, Cloud at FireEye

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.