Firebolt Case Study

Firebolt.com

Company size
50+ employees

Vertical
Big Data

Environments (cloud)
AWS

Key need
Runtime protection for detecting and auto-containing cloud attacks

Cloud security unlocked
0.04% false positive rate

About Firebolt

Firebolt is a data warehouse solution for low-latency analytics. It efficiently handles mixed analytic workloads, whether it's Extract, Load, Transform (ELT) processes or high-concurrency data serving tasks. What sets Firebolt apart is its seamless integration with SQL, providing users the simplicity and familiarity of querying data using standard SQL syntax while delivering exceptional speed and efficiency at scale.

Firebolt is an innovative data platform that empowers organizations to harness the full potential of their data by providing fast, scalable analytics solutions. Given that Firebolt hosts sensitive customer data, robust security measures are paramount—not just for their own operations, but for the protection of their clients as well. Runtime protection is crucial in this context, as it helps safeguard against complex and evolving threats in real time.

The Challenge - Eliminate White Noise and Focus on Active Threats

Before adopting Sweet Security, Firebolt faced substantial challenges with their previous technologies, particularly concerning excessive noise. The issue was not simply the quantity of alerts, as the number of actual incidents was relatively low, but rather the prevalence of false positives among those alerts.

This inundation made it increasingly challenging for their SOC team to differentiate genuine threats from false alarms in real-time, hampering their ability to respond promptly and prioritize remediation efforts effectively. Furthermore, delays in receiving alerts in near real-time compounded these difficulties, exacerbating the overall operational impact.

The complexity of managing these challenges highlighted Firebolt's urgent need for a more streamlined and effective runtime solution that could provide actionable insights without impacting performance. The chosen runtime sensor needed to be lean and practically unnoticeable to avoid degrading the performance of their core product. Nir Yizhak, the CISO of Firebolt, stated, **"We were clear that any solution we chose had to deliver security without compromising our operational efficiency".**

Precise Threat Detection and Minimal Noise

Sweet Security's ability to provide precise, actionable alerts aligned perfectly with Firebolt's commitment to proactive cybersecurity measures and operational efficiency. **"Sweet's ability to flag anomalies and categorize them as actual findings, without generating unnecessary noise, sets it apart from other solutions."**

Nir further explains the challenges of integrating new security tools, noting, **"Every new tool typically introduces noise as it learns and adjusts to the environment. However, with Sweet's ability to quickly baseline our operational model, there was no noise and we got actionable insights on day one."**

- ✓ **Detection & response**
- ✓ **Lean eBPF sensor**
- ✓ **Reduced false positive rate**

Lean eBPF Sensor that Never Compromises Performance

Firebolt recognized the need for a solution that not only reduces noise but also detects real, active threats without compromising operational efficiency. Nir emphasizes this point: "**Sweet Security's lean sensor has transformed our approach to threat detection. It allows us to focus on genuine risks while maintaining optimal system performance.**"

Sweet's lean sensor was built with cloud-native applications in mind, leveraging advanced eBPF technology to ensure performance remains unaffected, allowing organizations to operate seamlessly while still gaining comprehensive visibility into their applications and cloud environments.

"**Sweet Security's lean sensor is perfectly aligned with our needs, allowing us to maintain high performance while enhancing our cloud security.**" This emphasis on a lightweight solution was crucial for ensuring that security measures complemented rather than obstructed Firebolt's product capabilities.

Strengthened Defense with Sweet Security

Backed by rigorous testing from red teams, Sweet Security provides Firebolt with actionable insights and minimal false positives, ensuring their security and development teams can collaborate effectively without the distraction of irrelevant alerts. This robust approach enables Firebolt to strengthen their defenses while maintaining optimal performance across their operational environments.