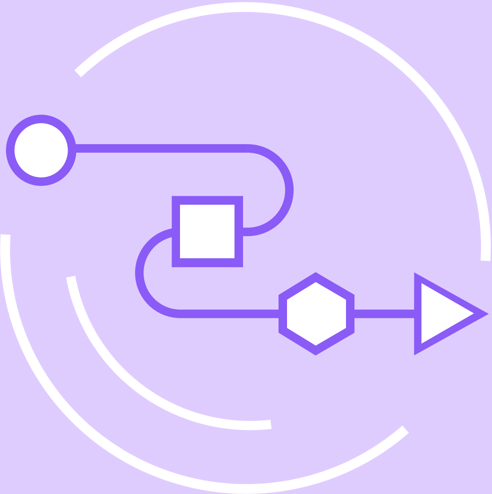
LEGIT



CASE STUDY

Customer Case Study: Firebolt

How Firebolt Uses Legit Security to Gain Visibility Into Their Application Security Posture from Code to Cloud

2025 Legit Security

Introduction

About Firebolt Analytics

Firebolt's mission is “to create the world’s most powerful cloud data warehouse and offer it as a service.” As a company that is “first and foremost customer-driven,” earning their customers’ trust is built not only on product innovation but on the confidence that Firebolt will do what it takes to protect their proprietary and sensitive data. Nir Yizhak, Firebolt’s CISO, is responsible for putting this into practice and was looking for a single solution to manage all of their application security activities, streamline their operations, and reduce the triage and execution time between issue discovery and remediation. He was looking for an ASPM solution that could integrate with the tools they already had in place and could adapt and grow with any future evolution to their environment. Also, Nir did not want to divert valuable engineering time and resources toward either an in-house or partial solution, which ultimately led him to Legit Security’s code to cloud ASPM solution.

> “When evaluating security tools, I’m trying to bring value and save engineering efforts.”

Nir Yizhak
CISO, Firebolt Analytics

FIREBOLT

Background

Informed decision-making, efficiency, and speed are not only central to Firebolt's platform but to their own internal SDLC and application security processes. At Firebolt, security is one of the company's top priorities, second only to innovation and delivery of the core product well. Nir Yizhak, Firebolt's CISO, is responsible for putting this into practice and was looking for a single solution to manage all of their application security activities, streamline their operations, and reduce the triage and execution time between issue discovery and remediation.

Firebolt was looking for:

- ▷ Broader coverage
- ▷ Better visibility
- ▷ Shortened triage times
- ▷ Improved collaboration
- ▷ Faster mean time to remediation
- ▷ Ease of deployment

Legit Security delivers business value

Legit delivered rapid value to Nir and his team, integrating with their entire toolset with minimal effort and providing immediate visibility into their application security posture from code to cloud. Once Legit was deployed, deep vulnerability and risk context was captured across their SDLC including existing security guardrails. This was supplemented by Legit's out-of-the-box security policies and remediation knowledge to give them the awareness they needed to intelligently prioritize issues based on business and security needs. That deep context, combined with the ability to automatically open, assign and track trouble tickets in their existing Jira deployment, allowed them to significantly shorten the duration time of application-related issues. Legit also gave them the tools they needed to provide important visibility into code/development cycle-related issues and remediation trends to the executive team. Ultimately, Legit Security gives Firebolt the single place they were looking for to orchestrate all of their ASPM activities.

Requirements

Prior to implementing Legit, Nir was relying on a tool that met some of his needs but imposed too many limitations to fit their long-term goals. In particular, it couldn’t cover all of the developer tools they were using and was unable to accommodate newly adopted code repositories or scanning tools they had recently migrated to. He was looking for an ASPM solution that could integrate with the tools they already had in place and could adapt and grow with any future evolution to their environment.

Required Integrations

- ▷ Software composition analysis (SCA)
- ▷ SAST
- ▷ Pipeline scanning
- ▷ Cloud scanning
- ▷ Jira
- ▷ Custom integration via API

Nir was ultimately looking for something that could collect, analyze, prioritize and track vulnerability and risk data across their entire pre-production development environment.

Digging In Deeper

How Firebolt selected Legit Security

Nir and his team are tasked with protecting Firebolt's large-scale, next-generation data warehouse that hosts a massive amount of customer data without slowing the software releases. In order to do this effectively, he needed to find a way to optimize not only the security team's time but to streamline communication and collaboration with Firebolt's software development teams. Nir understood that any solution he selected had to integrate with the tools that he already had in place and deliver the capabilities to manage, orchestrate, and control everything around the domain of application security.

While budget wasn't the main deciding factor in selecting the right tool, with a relatively small security team, any solution they chose had to be easy to implement and install and return immediate value. But first, it had to meet their core requirements.

Delivering value across the entire organization

Nir's security team (IT Security, DevSecOps, Security Research) is the primary user and manager of the Legit Security ASPM solution, using it to open tickets, analyze and prioritize risk, and track and govern all application security activities and issues. But in the spirit of transparency that has been embraced by Firebolt companywide, the engineering team has been granted access to the Legit solution as well. This not only makes collaboration between the teams easier, it gives the engineering team the autonomy and tools to prioritize and track their own work and fix potential issues before an alert is issued by security governance. Executive management also has access to critical KPIs from Legit, allowing them to stay on top of critical issues related to the code and development life cycle and delivering critical visibility into remediation trends.

Legit Security provides business value across the organization:

For application security teams:

- One tool to orchestrate everything related to AppSec
- Centralized issue tracking with all relevant context
- Out-of-the-box knowledge for better awareness
- Automates trouble ticketing and shortens issue duration

For software development teams:

- Visibility into potential risks before they become issues
- Ability to track issues across repos, developer activities and the pre-production development environment
- Helps developers stay on top of issues before escalation
- Streamlines communication and AppSec team collaboration

For executive leadership:

- Identify and track key risks to the software supply chain
- Executive visibility into code management and security processes
- Track remediation trends and continuous improvement efforts
- Build security awareness throughout the executive team

Summary

For Nir, Legit Security's value is easy to articulate to any organization that develops software and needs to add a layer of security control to their SDLCs. The more you leverage external services like GitHub in the SDLC, the more you expose your software supply chain and increase the probability of attacks. The faster you bring in an ASPM solution, the better protected your organization will be. For Firebolt, Legit Security was easy to deploy and very quickly gave them the broad and deep visibility into their application security posture that they needed. This saves a lot of engineering time that would have otherwise been wasted trying to maintain the several different sets of tools they would have needed without an ASPM.

About Us

Visit our website to book a demo and learn more about our platform at legitsecurity.com.
Get best practices on ASPM and software supply chain security from our blog.
Follow us on LinkedIn for the latest news, events, and resources.