Lightspin

An Industry-leader in Transportation Solutions Maximizes Productivity by Effectively Prioritizing Cloud Security Risks with Lightspin

"We've gone from 250 security alerts to being able to see the 10 critical ones for the first time. It's game-changing"

The Challenge

Too Many Security Tools, Creating Dozens of Alerts, and No Clarity

The company infrastructure:

Completely cloud-native and running on AWS. It has a complex infrastructure to secure, with one environment for R&D, and another for IT, and over 250 microservices, and all production activities running inside a Kubernetes environment.

Before Lightspin, our customer was challenged with:

- **A lean security team:** A relatively small security team among a large number of developers. It was important to ensure that developers could take responsibility over some part of securing the environment and that data security were freed up for ‘big ticket’ items.
- **Multiple security products:** With countless products to achieve a better security posture, the customer was seeing a high Total Cost of Ownership (TCO). It seemed that there was no way to effectively secure their environment with a single tool.
- **Alert fatigue:** As the company had so many security tools, this meant many alerts and warnings, all giving our dire warnings such as “high vulnerability” or “critical.” The developers were quickly switching off or ignoring the alerts. They needed to cut through the noise.
- **Human error:** Manual processes were prone to mistakes, and the customer knew that there was only so much they could achieve without automation.

“It's awesome to have a process but as long as there is no tool that knows how to enforce the process then the process is worth nothing.”

The Customer:

A global leader in corporate ground transportation, with extensive experience working with data and software applications.

The challenge:

Too many security tools, creating dozens of alerts, and no clarity

The solution:

Simplifying cloud security with Lightspin’s contextual prioritization

The results:

From 250 security issues, down to 10

The Solution

Simplifying Cloud Security with Lightspin’s Contextual Prioritization

The security team recognized that if you had dozens or even hundreds of items that were “critical”, you may as well be telling the executives that there are a thousand urgent items on the to-do list — none of them would be seen as important enough to get buy in. So they began to look for a vendor who could provide a solution that showed them what was critical.

The customer wanted a context-based understanding of their cloud, Kubernetes and microservices environment. After approaching Lightspin, the data security team were eager to move forward with a Proof of Concept (POC). Immediately, the customer could see things that had been missed by its existing security tools.

One example was demonstrated clearly with a widely-used developer platform, which had been up until this point considered trusted. Lightspin uncovered that it was requesting far too many permissions. It was creating risk in their cloud environment, and the customer could reduce the permissions to just what was needed.

When it came to risk assessment, while the customer's existing security solution had given dozens of security alerts, Lightspin was showing the customer actual risk, in language and structure that they could immediately visualize and understand.

> ***"Instead of sitting and scratching our heads, Lightspin tells me which of those many vulnerabilities is a top issue I must take care of now specifically and drop everything else. With Lightspin, we were able to focus on the top 10 images out of a file of about 250 images."***
>
> *Head of Security, a global leading transportation company*

The Results

From 250 security problems down to 10

- **A Secure Environment:** The developers have the tools and insight that they need to take control over their role in keeping the company secure.
- **True Visibility:** The data security team can now provide an accurate view of a complex environment from a single tool.
- **Reduced Risk:** No more alert fatigue, or sifting through data to find a real threat. Reports automatically isolate the vulnerabilities that matter.
- **Executive Visibility:** Data security can now tell executives exactly what's causing risk, and how to fix it, reducing the issues down to critical matters only.
- **Ready for Expansion:** As the customer moves towards its IPO, it has the peace of mind that its data is managed well and its processes are ready for scrutiny.

> ***"Lightspin helps me understand the prioritization of risk in my Kubernetes and cloud environments. Benefits include visualization and prioritization, knowing what's critical and what's simply unimportant, these are things that are priceless for us."***
>
> *Head of Security, a global leading transportation company*

About

Lightspin

Lightspin's contextual cloud security protects cloud and Kubernetes environments from build to runtime and simplifies cloud security for security and DevOps teams. Using patent-pending advanced graph-based technology, Lightspin empowers cloud and security teams to eliminate risks and maximize productivity by proactively and automatically detecting all security risks, smartly prioritizing the most critical issues, and easily fixing them.

For more information, visit: https://www.lightspin.io/