Lightspin | cherre

Case Study

Cherre reduces the noise and gets actionable insights with Lightspin's cloud native application protection platform (CNAPP)

Noise reduction and achievable, workable risk findings simplifies Cherre's ability to secure their multi-cloud environments

The Challenge

Building a robust security stack requires the right selection of tools, and the assurance that everything from dependency checks to having firewalls in place and meeting compliance requirements, are a part of the equation. As a startup in hypergrowth mode, Cherre's Security & Engineering team is lean, chartered with supporting the organization's dynamic growth and desire to get features and products to market quickly. Managing all facets of security well requires time and resources to ensure all areas are properly built and customized to the policies the organization requires.

For Cherre, they needed a tool that could help them easily scan their network for actionable vulnerabilities, so they could invest more time in the critical business issues that matter most.

"Continuous scanning from Lightspin across our network means that we are able to easily and quickly identify any critical gaps or vulnerabilities that could lead to potential exploits."

Stefan Thorpe
Chief Technology Officer at Cherre

cherre

Industry: SaaS, AI real estate data management

$50M Series B

Cherre is the leader in real estate data and insight. Cherre provides investors, insurers, brokers and other large enterprises with a platform to collect, resolve, and augment real estate data from thousands of public, private, and internal sources. By providing a "single source of truth," we empower you to evaluate opportunities and trends faster and more accurately, while saving you millions of dollars in manual data collection and analytics costs.

The Solution

Cherre quickly and easily integrated their Kubernetes environments through K8s templates provided by Lightspin, and within minutes were up and running on the system. First and foremost, Chief Technology Officer Stefan Thorpe saw right away that Lightspin wasn't cluttering his team with thousands of alerts, instead, a clear and easy-to-digest action item appeared right away – the number of critical attack paths discovered from the moment of initial scan.

"What struck me most about Lightspin was the fact that in the initial viewing of the Dashboard after we integrated our Kubernetes environments, instead of an insurmountable list of irrelevant CVEs, Lightspin presented maybe only tens of critical attack paths that were truly actionable. I don't need my team to see the 90-95% of the noise from non-critical alerts, I need only the truly exploitable risks that could do damage to the business."

Lightspin comes in, scans the network and highlights the gaps that exist. It reduces the time required from Cherre's internal team to curate the otherwise noisy systems they had and through Lightspin's root cause analysis tool, they have actionable dynamic remediation recommendations at their fingertips.

The Results

- **99% noise reduction**
- **100% visibility across multi-cloud and Kubernetes environments**
- **Clearly prioritized attack paths to bring focus to the team**

Lightspin

Lightspin is the #1 cloud security solution for SaaS companies of all sizes. Agentless and easy to deploy, Lightspin's Cloud Native Application Protection Platform (CNAPP) efficiently prioritizes and remediates cloud security risks in minutes thanks to the industry's only Attack Path Engine built on the graph. Supporting Amazon Web Services, Google Public Cloud, Microsoft Azure and Kubernetes, Lightspin simplifies cloud security and compliance via its self-serve offering and graph-based algorithms. Based in New York and Tel Aviv, Lightspin is backed by Dell Technologies Capital, IBM, and Ibex Investors. Leading companies such as ITV, PageUp, NEXT Insurance, and Imperva trust Lightspin to protect their data and workloads in the cloud.

To learn more, visit www.lightspin.io