sysdig

CASE STUDY

COMPANY DETAILS:

Beekeeper is the operating system for frontline businesses. With all communications, systems, and resources in one place, Beekeeper empowers frontline managers and employees to be more agile, productive, and safer in the workplace. The company believes in the potential of every employee and is dedicated to building secure, scalable technology that transforms how frontline teams, managers, and corporate offices work together.

BUSINESS NEED:

- Deliver a secure platform that protects customer data
- Provide remote, frontline workers with reliable applications

TECHNICAL NEED

- Gain insight into anomalous behaviors and potential threats
- Obtain visibility of cloud security posture and increase responsiveness to security and performance incidents

CHALLENGES

- Lack of visibility across security and DevOps workflows
- Targeting faster time-to-resolution
- Manual reviews and reporting was time intensive
- Reached an inflection point with Falco, needed more out-of-the-box functionality

BUSINESS IMPACT OF SYSDIG

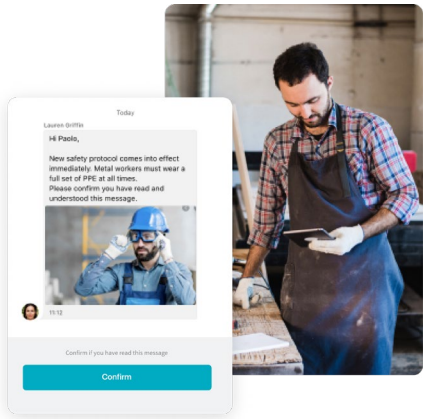
- Provides a single platform for security and DevOps teams to secure and monitor app health
- Gives the team confidence in their app security, enabling them to ship apps faster
- Pinpoints issues and potential threats faster
- Frees up engineering and security resources to focus on core business functions with automation
- Accelerates and streamlines compliance with simpler, more robust reporting

INFRASTRUCTURE

Amazon Web Services; Google Cloud Services Platform

ORCHESTRATION

Amazon Elastic Kubernetes Service (EKS); Google Kubernetes Engine (GKE)



Beekeeper Serves Up Secure Communications, Data, and Applications Across Cloud Environments

Overview

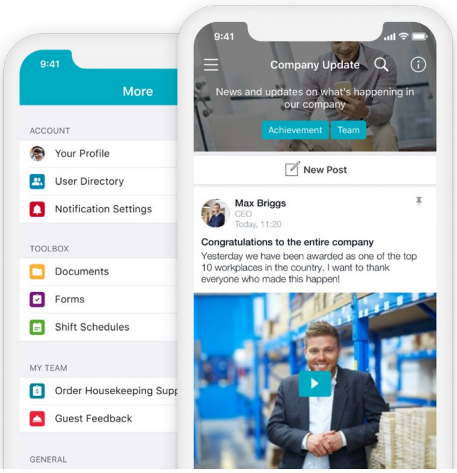
Beekeeper was created to help geographically distributed and remote workers stay connected to one another and to customers through its mobile and desktop platform. The company's applications enable secure information sharing between essential frontline workers, as well as deliver key communications and critical tools necessary for clients to succeed at the edge of their businesses.

"Every person that uses our platform demands a high-quality experience," says Michal Pazucha, Security Architect at Beekeeper. "Whether it's an HR manager delivering training across a distributed workforce or if employees in the field are filling out a customer intake form, things have to work flawlessly every time."

Security is top priority

Choosing to embrace DevOps practices, Beekeeper wanted to take a disciplined approach with how new

BEEKEEPER



functionality is added to its platform. Having clear visibility into how Beekeeper apps are operating, including uncovering misconfigurations, software vulnerabilities, compliance gaps, and anomalous activity before they become issues, is compulsory for creating the reliable experiences that customers demand.

A wide range of data is also being used across Beekeeper applications—from standard data collection forms to HR and proprietary information—so security is of paramount importance. The company wanted to proactively assess its cloud security posture, identify possible threats, and accelerate time to solution to meet compliance requirements and protect its clients.

"Security is our absolute number-one priority when it comes to creating and delivering unique employee experiences," says Pazucha. "As our customers are sharing and collecting information, we have to provide all of the safeguards necessary for them to function optimally and moderate risk as much as possible."

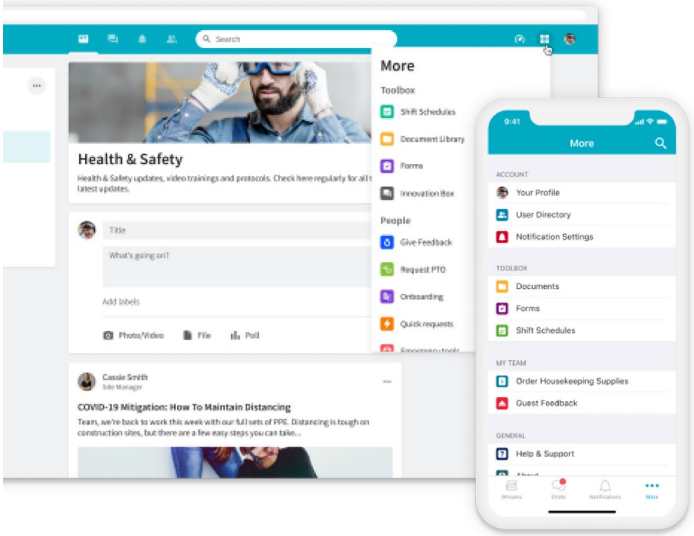
Adding to the challenge, the security solution Beekeeper chose needed to provide a unified view of risk across multiple cloud environments - AWS EKS and Google GKE are where its clients operate in, including Amazon Web Services (AWS) and Google Cloud Platform (GCP). Security alerts and context are often spread across multiple tools, which leads to inconsistent policies and an inaccurate picture of cloud risk. Before extending its apps into the cloud, the Beekeeper team realized the need for security throughout the lifecycle of its containers and recognized that visibility across their container and cloud environments was going to be key.

Enterprise Experience with Open Source Benefits

Early on in the company's security roadmap, Beekeeper relied heavily on open source Falco for visibility, real-time threat detection, and runtime security. "Falco is the de facto security solution. By using Falco, we knew we were adopting a standard for cloud and container runtime security. Being able to tap into the Falco open source community, and documentation was extremely helpful," says Pazucha. "Our Vice President of Technology, Filip Wieladek, also helped support our efforts to continue to evolve."

However, the company's environment became more complex as it migrated more services to multiple clouds. Beekeeper realized that it needed a managed, enterprise-class solution that could further automate security and visibility. Pazucha added, "We're big fans of the Falco project, but we reached an inflection point where we needed more out-of-the-box functionality to reach the security standards we've set for ourselves."

Transitioning from open source Falco to Sysdig Secure and Sysdig Monitor seemed like a natural progression for the Beekeeper DevOps and security teams. "We were familiar with the interface, the



libraries, policies, the community, the approach—everything about the Sysdig platform. It is based on Falco, so it was a safe bet," says Pazucha. "Falco's flexible syntax allowed us to create fine grained policies to accurately detect threats. At the same time, we were able to tune policies and create exceptions that ultimately reduced alerts in our environment."

"Seeing the Sysdig platform mature over time, combined with the backing of the security community, we were very comfortable with making the transition."

As the company evaluated security and monitoring solutions, Pazucha and team were extremely passionate about making sure its solution had open source roots. The team saw a major benefit in adopting a solution with a background in open source because of the cultural alignment between the two organizations.

"We're very collaborative with our approach as we work with our technology partners," says Pazucha. "Sysdig proved to us very early on that it was willing to work alongside us to support us, give us materials so we can continue to learn on our own, share insights through webinars, and help ensure we get the most out of the Sysdig platform, as well as help us meet all of our ongoing challenges."

Freed One Full-Time Engineer

Once the choice of Sysdig was made, Beekeeper quickly deployed the Sysdig platform with help from a Technical Account Manager. Nearly immediately, the company understood that it made a wise choice. "There are a lot of things that can go wrong in the cloud since we don't control everything," says Pazucha. "From a single pane of glass within the Sysdig dashboard, we can see what's going on in each cluster and be agile with how we identify and resolve issues across clouds."

Using Cloud Security Posture Management (CSPM) functionality within Sysdig solutions, the company can integrate cloud logs, like AWS CloudTrail and GCP Audit logs to get a better view of what's going on within its cloud environments. In addition, the company heavily relies on Kubernetes and containers to build and operate its SaaS solution. Beekeeper uses the managed Kubernetes offerings from its cloud partners including Amazon Elastic Kubernetes service and Google Kubernetes Engine. With Sysdig's unified approach, Beekeeper gains deep visibility into the activity and behavior across containers, Kubernetes, cloud services, hosts, and VMs using policies built on Falco.

"It's too tedious to go through logs and alerts manually to meet the standards we've established," says Pazucha. "It would require a full-time person, and is not a good use of time. Sysdig enables us to automate the entire process and reach a more accurate level of insight, faster."

Using Sysdig out-of-the-box rules, such as AWS Best Practices, Beekeeper can manage detection and alerts so team members can focus on the most important issues. For example, if an individual is

logging into an AWS console without using multi factor authentication, the Beekeeper team can quickly restrict access and investigate the issue.

From a monitoring perspective, the company also has a clear view into application metrics. "Sometimes, things just go wrong and we have to figure out the right approach to fixing them," says Karim Ouada, Software Engineer at Beekeeper. "Sysdig enables us to better understand the issue so we're taking the right approach—if we need to scale down the number of Kubernetes workers in the background, if we can see partitioning errors, if we lost some messages on a queue, and so on."

Ouada also added that having an audit trace through Sysdig enables engineers to shut down a cluster or a pod without fear of losing the data needed to understand an issue. "Previously, if we were to kill a cluster or a pod, we couldn't see what's happening. With Sysdig, we can respond to an issue quickly, while getting the insights we need to deliver a more secure, reliable solution through future audits–there isn't a compromise."

As a byproduct of audit tracing, enhanced visibility and added security features, Beekeeper has also dramatically accelerated and improved its compliance processes, including ISO27001, GDPR, HIPPA and the Swiss Data Protection Act , as well as successfully scanned more than 2000 images quickly as the log4j vulnerability was surfaced. "With Sysdig, it's simply night and day as to how quickly and accurately we can manage compliance," says Pazucha. "And even more importantly, we can save time and money, as well as avoid costs for being out of compliance."

Going Forward More Securely

As Beekeeper applications and systems continue to evolve, its DevOps and security teams plan to expand their use of Sysdig. In their DevOps workflows, teams see significant opportunities to continue to improve their applications, while security rules and processes proactively grow to outpace future challenges. At the same time, the Beekeeper team is confident that it has the right security partner in place that can scale as Beekeeper continues to grow.

"We're happy with the partnership we have with Sysdig and look forward to sharing insights, experiences and best practices, as well as continuing to learn from each other to keep security moving forward at Beekeeper," says Pazucha.

To learn more about Sysdig, visit www.sysdig.com or to try a free trial, visit www.sysdig.com/trial.

CS-BEEKP Rev. A 2/22