

COMPANY DETAILS:

Germany-based information extraction company that uses self-learned AI to automate data entry, such as invoices, receipts, travel expenses, and tax documents.

BUSINESS NEEDS:

- Stay ISO 27001 compliant
- Deliver secure applications internationally
- Ensure 'always on' platform availability

CHALLENGES:

- Limited visibility across bare metal and cloud environments
- Lack of data troubleshooting and compliance audits
- Limited activity monitoring and runtime policy enforcement

BUSINESS IMPACT OF SYSDIG:

The Gini operations and developer teams have confidence knowing their environment is secure. They are able to provide stable applications while saving time, allowing developers to focus on revenue-generating activities.

SYSDIG PLATFORM BENEFITS:

- Single tool across hybrid environment saves half a person on a two-person team
- Eases resource needs for proving compliance and audit exercises
- Developers are 20% more efficient
- Better informed capacity planning

INFRASTRUCTURE:

Hybrid: AWS Cloud and bare metal

ORCHESTRATION:

Kubernetes

Improving everyone's life by magically automating unpleasant tasks.

The Gini Way.



Gini Ensures Adherence to Strict EU Compliance Standards, While Reducing Dev and Ops Burdens

Overview

Gini is an information extraction company that automates the process of gathering information from financial documents. Based on self-learning artificial intelligence, Gini makes it easier to automate mundane tasks, such as invoice payments and other once-manual accounting tasks.

With millions of end customers, Gini's engineering team is responsible for maintaining a secure, 'always on' environment. The company operates 25 machines in an environment that spans bare metal and AWS Cloud. To ensure it can secure and monitor its hybrid cloud environment, Gini engineers rely on the Sysdig Secure DevOps Platform.

The Challenge

Originally built on bare metal, when Gini decided to transfer its development environment to the cloud, the operations team needed a way to reduce risk and ensure compliance. Gini manages highly sensitive user data, such as contracts and tax documents; therefore, complying with ISO 27001, an international standard for handling data that includes people and processes, is mandatory.

Case Study

Gini

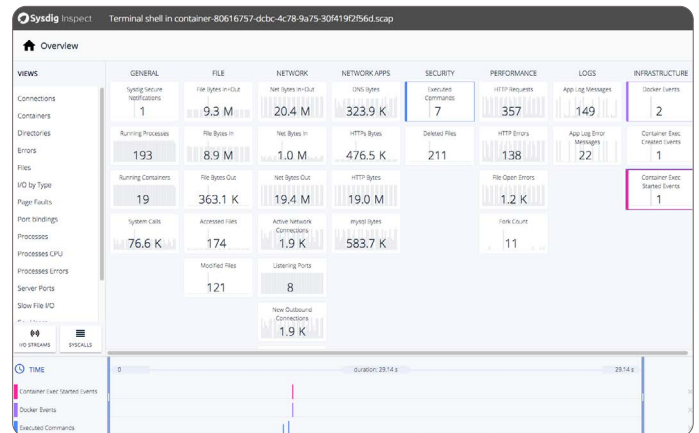
With multiple software updates a day, the team at Gini needed both visibility and security. According to Daniel Kerwin, Head of Technical Operations at Gini, their business depends on these apps. For his team specifically, the platform engineering team, they are responsible for providing “a stable and secure platform that allows our cross-functional product teams to create value for our customers at maximum pace with high confidence.”

25% operations savings: hybrid environment, single view

With a single agent, Sysdig provides security and monitoring across multiple environments, including bare metal, virtual machines, and cloud environments — AWS, Google, Azure, IBM, and VMware. Vendor lock in is not a concern because Sysdig works with all of the major cloud vendors to provide deep metrics across all environments. Being built on open source further strengthens integrations into the cloud providers.

According to Kerwin, “One of the most helpful things about Sysdig is that when I look at the dashboards, I get the same level of detail, no matter if I'm in the cloud or not. I don't have to go to a different tool to watch my AWS environment, it's a combined view. People don't really have to worry about if it's AWS today and Google Cloud tomorrow. It doesn't even matter because the Sysdig Secure and Sysdig Monitor views look the same, and this is a big benefit for us.”

Speaking about the benefit of having a single view across hybrid environments, Kerwin said, “Being able to move between our environments allows us to run faster. It's one tool for everything. It's not different tools optimized for specific environments. Having this single pane of glass, it doesn't matter where



it runs or how it runs. Compared to alternatives, Sysdig improves operations efficiency by 25% and developer efficiency by 20%.”

Simplified compliance

Gini uses Sysdig for compliance in a few ways. According to Kerwin, “From the compliance perspective three key things are important. The first are the runtime policies, the second is the activity model, and lastly, the ability to answer auditors’ questions.”

Proving a container did what it was supposed to do and nothing else, weeks, if not months, after the container is no longer running is impossible without a record. On its own, once a container is killed, there is no record. Sysdig helps organizations pass audits by capturing all container activity and correlating it with Kubernetes application context. This provides an audit trail that helps identify trends and prove compliance, even after containers are gone.

According to Kerwin, “We work with a lot of German banks and insurance firms, companies that are very data privacy sensitive. Being compliant with ISO 27001 is important to our business. Sysdig Secure plays a big role because auditors always

Case Study

Gini

have questions. 'How can you prove something happened? How do you know what people did? Can you prove it?' Sysdig Secure comes into play on a big scale when convincing the auditors. GDPR is also a concern in the industry. Sysdig helps us see and inspect operations that could interfere with GDPR in the end."

Developers are 20% more efficient

Before Sysdig, the Gini developers would have to check with the platform engineering team if they thought something was wrong. According to Kerwin, with Sysdig, "The developers are no longer waiting on us. They're doing their own thing. Our developers really like Sysdig. I always find it good when developers get used to a tool and they start to do their own things and feel ownership. In the early days, pretty much all monitoring questions ended up at my team. Developers were like, 'Hey, what's going on here? What's going on there?' And now they have their own team setups in Sysdig. They find their own stuff. I often don't even hear about it, they are self sufficient."

Further detailing how Gini developers use Sysdig, Kerwin explained, "Sysdig enables us to slice and dice our data to better understand our environment. Now I can't imagine a system where Sysdig doesn't exist. I really like that with Sysdig, we have an overview and then when I want to go down to the container level, I can use all these Kubernetes abstractions, like deployments or pods, and then switch in basically no time to the host and see the system in many different ways. This ends up being a 20% savings in time for our developers."

Troubleshooting from days to hours

According to Kerwin, "When things get really tricky, Sysdig Captures is the way to go for us to

"Being able to move between our environments allows us to run faster. It's one tool for everything. It's not different tools optimized for specific environments. Having this single pane of glass, it doesn't matter where it runs or how it runs. Compared to alternatives, Sysdig improves operations efficiency by 25% and developer efficiency by 20%."

- Daniel Kerwin, Head of Technology at Gini

troubleshoot. Sysdig Secure is still the only tool that can go back in time with the level of detail that it can." Sysdig Captures enable post mortem analytics. They capture all of the data on a container so teams can recreate total system activity, even for long-gone containers.

Detailing an issue his team had to troubleshoot, Kerwin explained, "One time we had to debug a network problem. We saw a network breakdown between two services and we couldn't explain it. It was an infrequent problem we were looking into it on and off for a few days. Once we decided to use Sysdig Captures, it only took us about two and a half hours to pinpoint the direction. The capture showed us that it was a DNS problem and it led us onto the right path. You look at it in hindsight now and say, 'Yeah, okay that was super obvious,' but it wasn't at the time and we used the Sysdig Inspect feature to really dig in."

Case Study

Gini

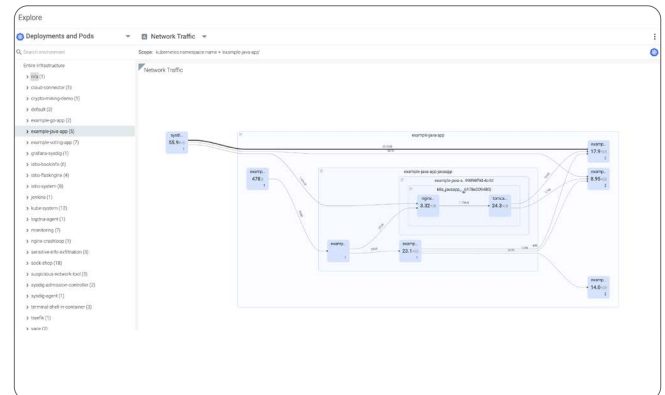
Deep visibility reduces after-hours work

When asked for the best advice someone transitioning to containers could receive, Kerwin explained, “I advise organizations new to containers to find something that gives real insights, that shows you things you haven’t seen before, and points out what you should look for. A tool like that makes your life easier and gives you confidence in your environment. This is what Sysdig Secure does for me. It gives me confidence that lets me sleep better. I really like the Sysdig integration with system calls. This enabled us to see what we couldn’t previously see. I suddenly had access to any view on my infrastructure.”

Without Sysdig, Kerwin explained, “We would know a lot less than we know today about our own infrastructure. We learned a lot when we added Sysdig four years ago. We had a lot less knowledge about what was going on then, a lot fewer insights, and there was a lot more after-hours work for me.”

“I really like the Sysdig integration with system calls. This enabled us to see what we couldn’t previously see. I suddenly had access to any view on my infrastructure.”

- Daniel Kerwin, Head of Technology at Gini



Ease of use with SaaS

Using the Sysdig SaaS solution significantly reduces Gini’s overhead. According to Kerwin, “I don’t have to worry about Sysdig. I don’t have to provide additional hardware, especially in the bare metal realm where you need time to order, it’s not so easy to have a lot of over capacity. By using SaaS, we don’t have to worry about that, which is definitely a plus for me.”

With the Sysdig SaaS solution, Gini has the advantage of getting access to new features faster with automatic updates, unlike a self-hosted solution. Kerwin noted, “Some vendors have large maintenance windows when making updates, or you never know when they update and if they update. We don’t have to worry about this with Sysdig.”

Better informed capacity planning

Understanding capacity and controlling cloud provider costs is often a challenge when operating in the cloud. With the information from Sysdig, Gini is able to make informed, intelligent choices about where and when to increase or decrease cluster resources based on factors like oversubscription.

Case Study

Gini

Kerwin's team uses Sysdig to see if his team has the right capacity reserved on AWS. As he explained, "When we calculate the resource requirements during load testing or something like that, we very easily see that with Sysdig. We can also see how close we are to our limits. That definitely helps. We can also take those numbers and put them into production, apply a little factor, and know how it will be when the real load hits."

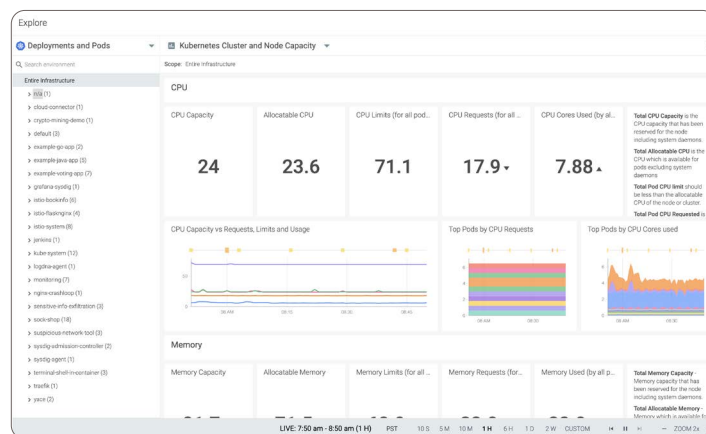
Being built on open source makes Sysdig stronger

Being built on open source projects is important to Kerwin, "I think giving back to the community is very important, and I also like Sysdig's open core model. For example, Falco is open source, people can contribute to it, they can use it in their own way, and then there's a product built on top of it. I think this is a good way to approach a security product. Sysdig makes a technology available that is valuable

to many people, even if not everybody is able or capable to pay a certain amount of money for that."

Kerwin expanded, "Continuing to use Falco as an example, the rule set gets bigger by people that are not employed by Sysdig as they see things in the wild. They write a request, put their merge requests or their pull requests up to the repository, and they make Falco better. When policies are contributed to Falco from the community, it in turn makes Sysdig Secure better. I think this is a good thing for the community and Sysdig users."

Sysdig is built on several open source projects, including open source sysdig, Falco, Prometheus, and Anchore Engine. Falco is the de facto open source runtime security project originally created by Sysdig, and is now a CNCF project. As Kerwin has seen, being built on open source enables Sysdig to innovate faster and gives companies confidence knowing they are standardizing on a community-backed standard.



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

