sysdig

CASE STUDY

Worldpay Gains Competitive Edge with Faster Delivery of Innovative PCI-Compliant Payment Solutions Globally

COMPANY DETAILS:
Worldpay by FIS is a Fortune 500, global merchant payment processing and services provider.

BUSINESS NEED:
- Easy-to-use, self-service security platform
- Security that can scale with FIS
- Reduce operational burden
- Streamline PCI compliance for merchants

CHALLENGES:
- Scalable visibility across cloud environments
- Lack of understanding vulnerability severity and remediation steps
- Limited audit trail for troubleshooting and compliance

BUSINESS IMPACT OF SYSDIG:
- Improved communication between DevOps and security teams in order to ship PCI-compliant apps faster
- Accelerated identification and remediation of vulnerabilities to avoid customer impact

SYSDIG PLATFORM BENEFITS:
- Reduced operational overhead by 50%
- Gained efficiency for troubleshooting and forensics with audit trails
- Achieved results in minutes with fast onboarding
- Reduced maintenance with a SaaS-first solution
- Simplified achieving PCI compliance

INFRASTRUCTURE:
Multi Cloud— AWS, Azure and Google

ORCHESTRATION:
Red Hat OpenShift

worldpay
from FIS

Overview

Worldpay by FIS is one of the largest global merchant payment processing and services providers. With billions of transactions annually, the Worldpay footprint spans 146 countries and encompasses more than 300 payment types in 126 currencies.

Their goal is to help merchants use technology to solve banking, payment, and investing challenges, as well as deliver superior experiences for their customers. Worldpay does this by building self-service, cloud-based platforms that make it easy for merchants to do business.

Challenge

As a major player in the ever-evolving payment business, Worldpay must innovate quickly to stay ahead of the competition. For example, when COVID-19 hit in early 2020, contactless payments — voice payments, retina-based payments, and digital payment mediums such as UPI, AePS, etc. — were reprioritized in an instant. To speed application build and delivery to meet changing demand, Worldpay utilizes a Red Hat OpenShift-based environment built on Kubernetes.

As an organization that helps merchants meet PCI compliance, ensuring uptime and security for applications is of critical importance for Worldpay. The company's developers need visibility into their various environments, which requires a security and observability solution that highlights potential issues across clusters and clouds.

According to Bernd Malmqvist, Principal Container Platform Engineer at Worldpay, “Sysdig has become an essential part of our offering and I think it's great to see that it really filled the gaps on both sides — the monitoring that development teams want to see, but also on the security side. Everyone has access to Sysdig and uses it.”

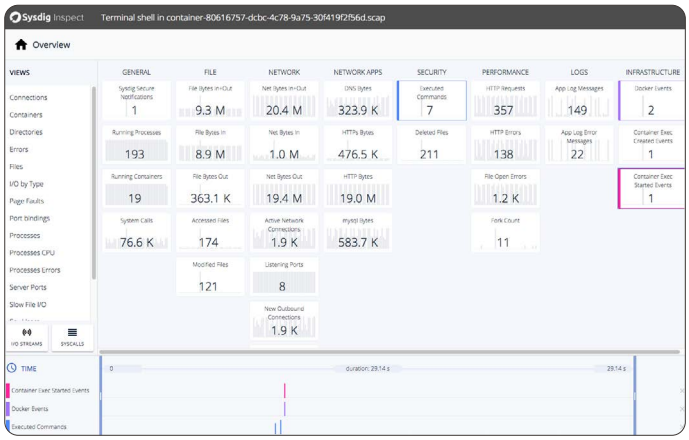
50% reduction in operational overhead

Worldpay likes the Sysdig SaaS-first approach. As Bernd explained, “We want 100% cloud usage. I have a massively dynamic infrastructure and I need it to always be available. I need it to scale and do it globally. We're heavily pushing the boundaries of how we build and deliver our platforms and I think Sysdig fits in very well in that type of model with its SaaS service. An on-prem data center is too restrictive and it's not dynamic enough, especially for us. Some of our customers do not have direct internet connectivity and an on-prem solution is too painful to actually manage in that situation.”

Bernd expanded, “We want to consume SaaS services where we can because it makes the operational overhead we have much easier, we just need to drop an agent. We don't need to maintain the backend, so our main focus is running our community platforms. For example, for us, we built our logic around cluster management, but we don't want to manage a Sysdig backend.”

According to Natnael Teferi, Lead DevSecOps Cloud Security Architect at FIS, with the easy onboarding, intuitive UI, deep data, and SaaS-first approach, “Sysdig reduced our operational burden by 50 percent.” As the only container and Kubernetes security solution built as a SaaS solution from day one, Sysdig is optimized for companies that want the flexibility that enables them to innovate quickly.

According to Bernd, "We're trying to get to the point where we deploy these clusters and we have zero effort operating them, because they can operate themselves. Sysdig is helping us get there. Sysdig is pushing the boundaries, just like us. They are constantly pushing the roadmap and delivering new features. With Sysdig, we're not scared of using new features made available. Sysdig just works and we trust in the product."



Took PCI compliance off of our plate

As a payment processing platform, PCI compliance is a huge hurdle for Worldpay. As applications migrate to the cloud, container sprawl and short container lifespan make PCI compliance challenging. Validating compliance is the number one blocker for faster application delivery. A failure to meet compliance could result in massive fines, but even more significant, a loss in customer confidence and revenue.

As Bernd put it, “PCI compliance is one of the biggest challenging factors for running a Kubernetes

platform in a high-security environment. Sysdig made our life easier because it just reduced the effort on our side and made the PCI element simpler. There's a lot of work in building a secure platform, but when it comes to certain elements — prevention, runtime analysis, intrusion detection, vulnerability scanning — having Sysdig just stops the conversation around PCI."

Security, DevOps and operations work as a team

Running containers and Kubernetes in production requires security and visibility that integrate into existing workflows. Sysdig is the only solution that can address security, compliance, and monitoring use cases with a single agent and backend, which was really important to Worldpay. Beyond tool consolidation and cost savings, Worldpay is able to address several use cases with less drain on resources.

According to Natnael, "We operate a distributed platform, so having one tool that addresses several security and monitoring use cases is wonderful. The single agent that is non-intrusive means we do not have multiple agents that could interfere with each other."

Bernd expanded, "My team works very closely with Natnael's team, so having Sysdig Monitor and Sysdig Secure without adding an additional agent was really quite impressive for me. Other solutions we've used are very intrusive into an OpenShift platform and that caused issues in the past at Worldpay. I think having that single, non-intrusive agent is very important."

> **"With the audit log inside our S3 buckets, we gain full visibility of activity, enhancing our monitoring and investigative capabilities. Having this information saves so much time, because without the audit trails, how do you know what happened? Other solutions do not offer this."**
>
> **- Natnael Teferi**
> **Lead DevSecOps Cloud Security Architect**

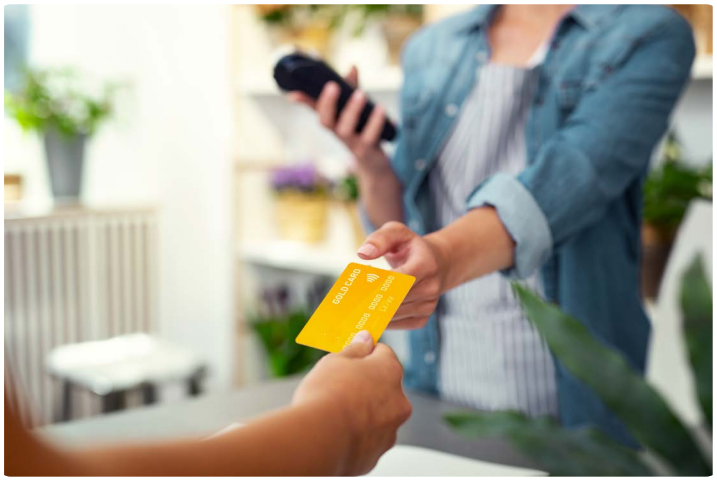
Audit logs make forensics a possibility for the first time

When it comes to incident response for Kubernetes, SOC teams need to be able to analyze an endless list of scenarios. In container environments, when the container is gone, so is its data, making forensics nearly impossible. Having data available to speed incident response is an invaluable insurance to have when something goes wrong. "The forensics functionality was key for us in selecting Sysdig for security. With the audit log inside our S3 buckets, we gain full visibility of activity, enhancing our monitoring and investigative capabilities. Having this information saves so much time, because without the audit trails, how do you know what happened? Other solutions do not offer this. Beyond that, Sysdig will help identify who needs to be notified and with lessons learned from the configurations," said Natnael.

Natnael expanded, “The lifecycle of the container is measured in seconds, and there is a high degree of variety of how you're going to make things happen, especially for the security team. We need to be able to count on the security and the integrity of containers that may be online for a few seconds, maybe a few weeks, and then they are disappearing. With Sysdig, we have real-time visibility across the whole FIS environment. Then if something happens, we still have that data to investigate with.”

Spend time on revenue producing work, not managing risk

According to Bernd, Sysdig doesn’t inundate his team and customers with unimportant information. Instead, Sysdig does the work to show only what is important. “When you use a container security tool, everyone knows that once you deploy and it's connected to the backend, you log in, and suddenly you get an overflow of information about your containers, indicating they are all vulnerable. It’s so daunting and you don’t know where to start. What I liked with Sysdig is that when you log in, everything is mostly green. The experience using Sysdig is so much more user friendly because logging in doesn’t feel like a hammer hitting your heart, making it look like your system is in extreme danger, when in reality, most of them are minor vulnerabilities. I am usually interested in the high or severe vulnerabilities, and that is what Sysdig shows you when you use the dashboards. You can easily get all of the information on the minor vulnerabilities as well, but the majority of time, you aren’t interested in that, right? So I don’t want to wade through that, I just want to be shown what I should care about, which is what Sysdig shows us.”



Natnael went on to explain, “From the security point-of-view, if we identify a number of vulnerabilities and the Dev team is working in an agile manner, they may well have planned certain times of the week to fix vulnerabilities. If my team logs in and sees 500 vulnerabilities, they then think, ‘am I going to fix our vulnerability or am I going to spend my time developing something which creates some money.’ Sysdig will highlight for you where the fixes are available. This is so helpful, my team can easily fix the image and move on. Showing us what is important and how to fix it is key to reducing our risk, the tool doesn’t waste our time.”

When it comes to setting policies to manage risk, Natnael said, “With Sysdig’s runtime policy functionality, we can easily create a policy and that immediately creates a notification alert. It's very simple to work through the policies, as well as the deployment. We just create some kind of daemonset. That, along with the guidance from Sysdig that outlines how to deploy different scenarios, makes it really easy to manage our risk.”

Full Prometheus compatibility

Many developers start with open source Prometheus in order to obtain key metrics for cloud-native services; however, scaling in production with multiple Kubernetes clusters requires multiple Prometheus servers, making it difficult to view trends. Issues on microservices that have cross-platform dependencies can easily go unnoticed. For Worldpay, Sysdig's use of Prometheus and the PromQL language is a huge benefit.

According to Bernd, "My guys are very happy with Sysdig because we are heavily making use of Prometheus and they like Sysdig's support for PromQL. It's essential for us actually. We have built so much around Prometheus, and with Sysdig, we are able to really use those metrics. One of our next projects is continuous delivery with multi-region implementations, and this is where Prometheus will be really important. Sysdig's support of Prometheus is unique and it is definitely at the top of the list of what will help us build more tooling around these platforms.

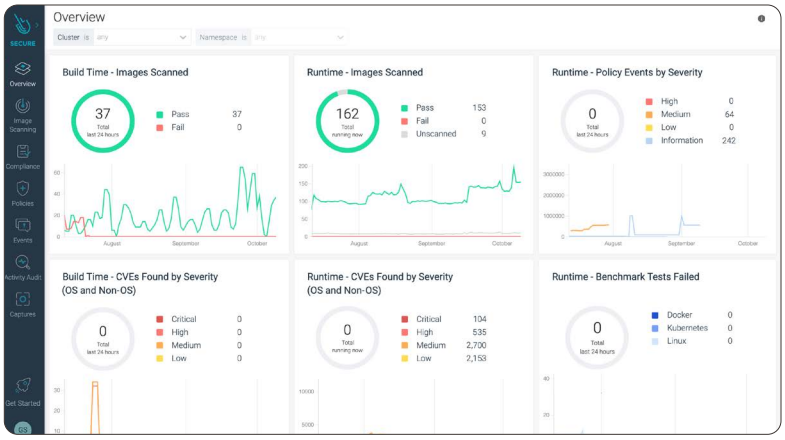
Up and running in 30 minutes

With developers around the world using the self-service platforms from Worldpay, onboarding of any tool is extremely significant — after all, time is money. One thing customers like Worldpay love about Sysdig is how quickly they can onboard and start getting results.

According to Natnael, "Installing Sysdig is quick and easy. You don't have to implement a GUI or open firewalls, which with that type of implementation is costly. Getting Sysdig SaaS up and running basically took 30 minutes until the first cluster provided metrics. Compared to other tools we used previously, it took us a month to get to the same point. Sysdig comes with great out-of-the-box policies, which saves us loads of time."

The easy-to-use Sysdig Teams feature enables admins to control who has access to what, which is important to Natnael. "Going forward, after installation, when we add new teams that need access, we just assign one team manager. The team manager has the ability to distribute access and manage their teams, so that is another cost where we save. People aren't wasting your time asking for access and logins, but rather they're going to the team manager and they just organize who should have access and who should not."

> **"We're trying to get to the point where we deploy these clusters and we have zero effort operating them, because they can operate themselves. Sysdig is helping us get there."**
>
> **- Bernd Malmqvist**
> **Principal Container Platform Engineer, Worldpay**



Sysdig makes multi-cloud possible

Between FIS and Worldpay, the infrastructure supporting their applications spans several clouds. According to Natnael, "FIS adopts a truly multi-cloud ethos, so it is paramount to provide the security and monitoring functions in a cloud agnostic manner. As the company continues to grow, Sysdig is playing a big role because Sysdig will support all platforms for us. If FIS purchases another company within a couple of years, we can just easily expand our Sysdig security and monitoring tool across when a new company joins. This simplifies the deployment, reduces the time to integrate, and subsequently secure the new acquisition."

Sysdig is an active member of the open source community

Sysdig is an open source-based company that has contributed several products to the community, including Falco, the de facto cloud-native runtime security project that was adopted by the CNCF. Sysdig is helping set best practices and doing its part to help the community. Being built on open source also enables Sysdig to innovate faster.

According to Bernd, “I really like that Sysdig is so active with open source. Sysdig has open source projects for both security and monitoring. People can deploy both and run them for free. Then there is an enterprise version that fits nicely once you progress through the open source tools. If you need more capabilities and features, Sysdig is there for you. Being a good community member and driver is important to me.”

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

CS-WORLDPAY Rev. A 1/21