sysdig

CUSTOMER STORY

Data Notebook Company Supports Compliance and Shuts Down Advanced Attacks

Organization Chooses Sysdig for Vulnerability Management and Container and Cloud Security

With a simple mission to make data accessible, usable, and valuable to everyone, this company's cloud-based collaborative data notebook blends business intelligence, project management, and AI-driven analytics.

To that end, the platform is incredibly versatile, supporting no-code visualization and data exploration while also allowing businesses to execute their own code in languages such as SQL, R, and Python.

Data Notebook Company

INDUSTRY

Business Intelligence / Data Analytics

CHALLENGES

- Difficult to ensure SOC 2 compliance across a complex cloud environment
- Exponential increase in cryptomining activity
- Risk of security operations negatively affecting legitimate users

OUTCOMES

- Audit logging helped ensure seamless SOC 2 Type 2 compliance
- 60+ cryptomining exploits blocked per day; 99% reduction in time spent addressing malicious activity
- 20 times increase in user signups while simultaneously improving security

CHALLENGES

Cluster Security, Compliance, and Convenience

When the organization approached Sysdig in 2022, they sought a vendor that could help them achieve SOC 2 Type 2 compliance. Although a small company at the time, their platform was anything but. Hosted on Amazon Web Services, the company's infrastructure totaled 83 nodes across six environments.

They used this infrastructure to support three different deployment models: multitenant, single tenant, and managed.

Because the company lacked dedicated security and compliance teams, management of both fell to their DevOps team. Consisting of just four engineers, the team was also responsible for infrastructure, deployment, and maintenance. The company evaluated **Sysdig** alongside competitors, with Sysdig eventually winning out for several reasons.

"During the demo with Sysdig, I remember being impressed at the platform's ability to visualize and map network traffic," said the company's senior DevOps engineer. "For SOC 2 compliance, it was also important for us to have vulnerability scanning, audit logging, and runtime security. Sysdig provided these features out of the box, along with a way to demonstrate these capabilities to auditors."

"I was also looking to create automated network policies for our clusters," she said. "That was something else Sysdig did very well. Its deployment model was also best aligned with our practices, as was its pricing model."

The decision was made; the choice was Sysdig.

It turned out, however, that compliance and visibility weren't the only challenges the company faced. After choosing Sysdig and with the release of their public beta in 2022, users were free to execute arbitrary code through the platform. This made the organization an ideal target for cryptominers.

> "Cloud security and compliance are incredibly challenging without dedicated in-house professionals – but Sysdig has made it easy for us to elevate our DevOps team into handling both. Container security, vulnerability scanning, audit logging and runtime security are now routine tasks with minimal impact on the team's workload."
>
> **Senior DevOps Engineer**

Stopping Cryptomining Dead in Its Tracks

“The first few weeks were kind of low impact for us,” the DevOps team lead said. “We saw a few cryptominers that occasionally ran kernels for a few hours, so we created some basic monitors. At the time, it was easy for us to manually terminate malicious containers.”

Unfortunately, that soon changed. As the company grew more popular, cryptomining activity on the platform increased exponentially.

“We went from three or four malicious users per week to more than 60 per day,” she said. “Identifying and blocking them became a full-time job for my team, and we eventually needed a dedicated person to terminate cryptopods. Worse, by the time we investigated and terminated one malicious container, 10 more took its place – it was a never-ending game of whack-a-mole.”

The company couldn’t afford to allow cryptomining to tank performance for their users – doing so could potentially cost the company tens of thousands of dollars. At the same time, they couldn’t risk killing legitimate containers with false positives.

With the recent onboarding of Sysdig, the DevOps team configured the Sysdig platform with a set of cryptojacking-focused rules and policies. Less than a week later, all cryptomining activity on the platform had ceased.

“We were impressed with how effective Sysdig’s rules were for detection,” the DevOps engineer said. “Our team worked very well with the Sysdig Threat Research Team, sharing insights as cryptominers kept trying to fly under the radar. I think we even discovered some new attack methods at one point.”

> “We experienced a 20% increase in users nearly overnight and expected a surge in cryptomining activity – thanks to Sysdig, that surge never occurred”
>
> **Senior DevOps Engineer**

SOLUTIONS

Preventing Exploits at Any Scale

When the company released a ChatGPT plug-in, they experienced a massive influx of new users. Anticipating that such growth would result in renewed cryptomining activity, they braced themselves for a flood of attacks. However, it proved a non-issue – the organization didn't even need to adjust its policies.

"We experienced a 20% increase in users nearly overnight and expected a surge in cryptomining activity – thanks to Sysdig, that surge never occurred," the DevOps engineer said. "The same rules and policies we originally implemented continued to work as expected. They scaled up with no impact to our platform, which was really amazing."

> For SOC 2 compliance, we need vulnerability scanning, audit logging, and runtime security. Sysdig provides these features out of the box."
>
> **Senior DevOps Engineer**

> There's no recipe for how to mitigate cryptomining and cryptojacking. We're really thankful for our partnership with Sysdig."
>
> **Senior DevOps Engineer**

A Partnership Built on Trust and Support

When the company first approached Sysdig, their use case was relatively straightforward. They needed to support their SOC 2 compliance efforts with audit logging, policy management, and vulnerability scanning.

Since leveraging Sysdig to address cryptojacking, the company was delighted to discover the additional benefits of working closely with Sysdig's team.

"Cloud security and compliance are incredibly challenging without dedicated in-house professionals – but Sysdig has made it easy for us to elevate our DevOps team into handling both," the engineer said. "Container security, vulnerability scanning, audit logging, and runtime security are now routine tasks with minimal impact on the team's workload."

Data Notebook Company

INDUSTRY

Business Intelligence / Data Analytics

INFRASTRUCTURE

AWS

ORCHESTRATION

Kubernetes

SOLUTION

Sysdig Secure

About Sysdig

In the cloud, every second counts. Attacks move at warp speed, and security teams must protect the business without slowing it down. Sysdig stops cloud attacks in real time, instantly detecting changes in risk with runtime insights and open source Falco. We correlate signals across cloud workloads, identities, and services to uncover hidden attack paths and prioritize real risk. From prevention to defense, Sysdig helps enterprises focus on what matters: innovation.

Sysdig. Secure Every Second.

To learn more about Sysdig, visit **sysdig.com.**

REQUEST DEMO →