sysdig

CUSTOMER STORY

Health Care IT Org Achieves Compliance, Reduces Computing Costs 30%

A full-service IT company, this organization gained recognition with its award-winning state-based marketplace (SBM) platform. Built in the cloud, the platform provides those in search of health insurance plans interactive features such as plan comparisons, a cost estimator, and doctor lookup tools.

“Our solution allows thousands of otherwise uninsured individuals to gain easier access to health care and financial assistance via government programs,” said the organization’s senior cloud security and DevOps engineer.

The company’s platform has helped states like Maine and Massachusetts map their disparate data sources into single, integrated technology engines, decreasing costs and improving coverage. But as any developer will tell you, with government-aligned programs and faster software rollouts come more rigid compliance requirements and more software vulnerabilities, both of which were top of mind when the organization began looking at Sysdig.

Health Care IT Org

CHALLENGES

- Time-consuming, manual compliance checks
- Alert overload from noisy vulnerability alerting
- Ensure that information security policies exceed MARS-E 2.0 industry standards
- Lack of audit trails for post-incident forensic investigations

OUTCOMES

- >10 hours saved per week auditing infrastructure
- 98% reduction in vulnerability noise
- 30% reduction in computing costs
- <1 minute to achieve IAM posture, saving 4+ hours per week

CHALLENGES

It's Not What You Don't Know...

As the organization began to build cloud-based software for state governments that were also federally compliant, they quickly ran into cumbersome compliance processes and a laundry list of vulnerabilities. "It's not what you don't know that gets you into trouble," said the cloud security DevOps engineer, paraphrasing Mark Twain. "In the security world, it's what assumptions were made during the process of building software that are not true and can be exploited." Real-world implementations can often differ substantially from the intended, secure designs and may exhibit exploitable security conditions that put data at risk.

The company handles personally identifiable information (PII) and protected health records (PHIs), making compliance a critical focus. While working toward compliance in its cloud environment, for example, they needed to meet 250 different controls, including those from the National Institute of Standards and Technology (NIST) SP 800-53, each of which took about 30 minutes to validate; more than 125 hours were spent mapping each control manually.

Even more concerning was the lack of insight into its cloud-native workloads. Ultimately, they could scan code and fix misconfigurations during build but had little context for what was happening during runtime. These concerns were compounded by the ephemeral nature of the containers themselves – how were they to audit or conduct forensic investigations on these workloads long after incidents had occurred?

So, with an eye toward open source and a desire to automate processes, they sought out a platform that could bring security and observability together.

> "Using Sysdig runtime insights to identify the vulnerable packages that are in use has netted a 98% reduction in vulnerability noise. Reducing vulnerabilities from 500 to just 10 is amazing, and rapidly elevated our security posture."
>
> **Senior Cloud Security and DevOps Engineer**

SOLUTIONS

The Sysdig Difference: Cost Savings and Tool Consolidation

In its early days of cloud adoption, the company attempted to meet its requirements using a number of open source tools. Constrained by budget, their cloud security team spent the better part of a year collecting metrics and exploring the extent to which their deployment velocity was hindered by manual processes.

“We had a successful trial run, and at the end of the year we had a very good idea of how much effort was put into achieving security, compliance, and even monitoring,” the cloud security DevOps engineer said. “However, prior to Sysdig, a significant amount of human capital was required, incurring its own set of costs.”

Many compliance and risk teams can sympathize, as they often struggle to keep pace with the rapid software release cadences. The pace only accelerates as organizations undergo digital transformation.

“After comparing our manual solutions with the cost of Sysdig for one year, we chose Sysdig – and are very happy we did,” he said. “Now, one tool can achieve what previously required six tools, resulting in savings exceeding Sysdig costs.”

SOLUTIONS

Process Automation and Continuous Compliance

Because the organization has access to personal data and health records, they must be compliant with Minimum Acceptable Risk Standards for Exchanges (MARS)-E 2.0. Additionally, the company self-imposed other standards, such as NIST SP 800-53 for security and privacy controls, NIST 800-190 for application security, and NIST 800-204 for microservice-based applications, all of which are supported and effectively mapped by continual compliance validation within the **Sysdig** platform.

Sysdig provides out-of-the-box compliance checks for container and Kubernetes environments that offer an instant snapshot of compliance postures, highlighting each passed and failed control. “Instead of manually running an audit of the infrastructure, then analyzing and prioritizing the findings, we use Sysdig,” the engineer said. “It improves our security posture and saves us one hour a week per cloud environment per standard – about 10 hours per week in total.”

“And Sysdig captures detailed container forensics data that serve as proof of compliance for third-party auditors even after containers are gone,” he continued. “We are much less afraid to be ephemeral, and this is invaluable.”.

> “After comparing our manual solutions with the cost of Sysdig for one year, we chose Sysdig – and are very happy we did. Now, one tool can achieve what previously required six tools, resulting in savings exceeding Sysdig costs.”
>
> **Senior Cloud Security and DevOps Engineer**

SOLUTIONS

Improved Security Posture

In the past, triaging all of the security findings was a challenge for the company. Various scans used previously produced an unmanageable slew of false-positive vulnerabilities that required manual prioritization. The ability to prioritize vulnerabilities using runtime insights from Sysdig has become a critical feature.

Sysdig helps organizations improve their security posture by focusing on the vulnerabilities, misconfigurations, and compliance gaps that create the greatest risk. The platform enables cloud security teams to identify threats to health insurance customers and their data in real time, prioritize relevant vulnerabilities, and swiftly address them with contextual information, thereby minimizing the risk of incidents or breaches.

“Using Sysdig runtime insights to identify the vulnerable packages that are in use has netted a 98% reduction in vulnerability noise,” the cloud security DevOps engineer said. “Reducing vulnerabilities from 500 to just 10 is amazing, and rapidly elevated our security posture.”

“With Sysdig, we’re able to ensure the limited resources in our organization have the maximum impact in improving our overall security posture,” he said.

Even beyond a greater security posture, the company was empowered by more granular historical data about every resource in its cloud environment. “One of the Sysdig features I really love is container drift control,” the cloud security DevOps engineer said. “With **drift control**, I can be alerted if there is a file creation or modification in the container. I can then initiate a forensics capture or even stop that container. It has proven to be very useful.”

“The identity and access management posture within the Sysdig platform also brings increased awareness and allows us to spend less time going through access logs,” he said. “We can achieve at a glance what used to take a couple of hours twice a week.”

SOLUTIONS

Optimizing Performance and Reducing Costs 30%

To improve cluster capacity planning, track how its applications are running on Amazon Web Services Elastic Kubernetes Service, and control cloud expenses, the company's security team also uses **Sysdig Monitor**. Operating from the same agent and software-as-a-service back end as Sysdig Secure, Sysdig Monitor radically simplifies cloud and Kubernetes observability and helps lower the costs associated with gaining deep visibility into cloud-native workloads.

"I love looking at my dashboards every morning," the cloud security DevOps engineer said. "I can see things like resources and request limits and perform pod right-sizing and workload capacity optimization."

With Sysdig Monitor, the organization can look back in time and compare details, such as the number of resources used month to month. In addition, during peak periods like open enrollment, the company gains insight into how much they need to scale to service the required traffic.

Using Cost Advisor within Sysdig Monitor, the company is also able to look at fine-grained details and discern how much each namespace, pod, and workload is costing the company. "With the implementation of the Cost Advisor recommendations, we project a 30% savings in computing costs alone in the coming year," he said.

> “ With the implementation of the Cost Advisor recommendations, we project a 30% savings in computing costs alone in the coming year."
>
> **Senior Cloud Security and DevOps Engineer**

Decreasing Time to Market, Increasing Revenue

As a key technology provider, Sysdig facilitates the organization in advancing security measures earlier in the development process, enhancing deployment speed, reducing downtime, and boosting revenue. This collaboration enables the company to confidently undertake additional projects.

The cloud security DevOps engineer highlighted the comprehensive benefits, concluding, “With Sysdig, we enhance our solution’s security, scale up effectively, and actively seek new business opportunities, from high-level security policies to runtime anomaly detection.”

Health Care IT Org

INDUSTRY

Health Care / Business Services

INFRASTRUCTURE

Amazon Web Service (AWS)

ORCHESTRATION

AWS Elastic Kubernetes Service (EKS), Microsoft Azure Kubernetes Service (AKS)

SOLUTION

Sysdig Secure, Sysdig Monitor

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 →

sysdig

CUSTOMER STORY

CS-HEALTHCAREIT
REV. A 4/24