sysdig | AUTOMOX

CUSTOMER STORY

Automox Cuts False Positives by 80% and Boosts Vulnerability Response Speed by 30%

Founded with a mission to empower IT operations teams, Automox provides a powerful, intuitive solution for managing and securing endpoints across diverse operating systems, from Windows and macOS to Linux. Its platform enables IT professionals to streamline patch management, software deployment, and compliance enforcement – all from a single, centralized console. Trusted by companies of all sizes, Automox automates critical tasks and delivers real-time insights to help businesses enhance cybersecurity, reduce operational complexity, and achieve unparalleled efficiency.

AUTOMOX

INDUSTRY

Software Technology

CHALLENGES

- Difficulty securing Kubernetes workloads given limitations of the existing EDR solution
- Limited visibility into container vulnerabilities and AWS environments
- Complexity of maintaining compliance with regulatory standards such as SOC 2

OUTCOMES

- Reduced false positives and streamlined security operations by leveraging Sysdig's customizable detection and response rules
- Built a more robust vulnerability management program using Sysdig's runtime insights and reporting capabilities
- Strengthened compliance efforts by conducting a full identity and access management (IAM) audit and building a secure image pipeline with Sysdig's tools

CHALLENGES

Navigating Noise and Blind Cloud Spots With a Traditional EDR Tool

Automox encountered several challenges in securing its Kubernetes environment. Their existing security solution, initially chosen for its endpoint detection and response (EDR) capabilities, fell short when deployed in Kubernetes clusters. The platform generated excessive false positives, wasting valuable security practitioner time and making it difficult to discern real threats. Additionally, its configuration and management demands were so high that they placed a significant burden on the team.

"The platform turned into a false positive factory when we deployed it into our clusters," said Mat Lee, Senior Security Engineer at Automox. "It was also very hard to tune and make exceptions, so configuration and management was a full-time job. We decided to retire it, and I was tasked with finding a replacement."

The lack of deeper visibility into Kubernetes clusters compounded the problem. Automox needed a solution that could not only reduce noise but also provide actionable insights to guide vulnerability management efforts. This was critical given the sensitive nature of their operations – Automox's agents had root-level permissions on customer devices, making any potential compromise a severe risk.

"Our primary focus when we started looking for a replacement was to get greater visibility into our clusters," Lee explained. "Because of the nature of our agent, which is deployed on customer systems, we needed a holistic and full-coverage solution to protect the assets that back our product."

Automox's journey to find a replacement solution highlighted the growing importance of cloud-native security tools designed specifically for Kubernetes environments.

> "Sysdig stood out for its ease of use – our team adapted quickly, and the built-in rules worked so well that only minimal customization was needed."
>
> **Mat Lee**
> Senior Security Engineer, Automox

CHALLENGES

Cutting Through Cloud Security Vendor Hype

Over the course of three months, Lee and the Automox team evaluated about seven different vendors in their search for a robust Kubernetes security solution. The results, however, were less than promising.

This frustrating experience highlighted the disconnect between vendor promises and actual product capabilities. The journey underscored the importance of finding a partner whose solution could deliver on its claims and align with Automox's technical and budgetary needs.

"The experience with the Sysdig team was genuine and a partnership from day one," Lee said. "From our first conversation and demos to the ongoing support we receive today, there are no hidden tricks. It's just great technology backed by a great team that wants to partner with their customers in the fight against bad actors."

> A lot of vendors boasted about advanced threat detection with protection from code to cloud. But once we jumped in, their actual products looked completely different from their marketing and initial sales calls. I even wondered if we were missing something – like maybe a feature flag hadn't been activated."
>
> **Mat Lee**
> Senior Security Engineer, Automox

SOLUTIONS

Falco's Flexibility, Sysdig's Simplicity

"**Falco** was what inspired us to ultimately choose Sysdig," Lee said. "I've worked with Falco for a couple of years, and it offers both the flexibility and extensibility that we need. There's no smoke and mirrors – when you look at a Falco rule, you know exactly what it's doing."

Ease of use was another key factor in Automox's decision. According to Lee, the team quickly adapted to the **Sysdig Platform**, and feedback has been overwhelmingly positive. One team member even took the initiative to become a dedicated detection engineer, creating custom rules tailored for Amazon Web Services (AWS) and Kubernetes.

"Another of our engineers has been exploring threat-hunting frameworks to test Sysdig's out-of-the-box alerts in our environment," Lee said. "So far, they've only needed to make a few custom rules. Everything else has been effectively managed with the default rule set. Other solutions require considerable resources to ensure that we're protected against new and emerging threats – **Sysdig's Threat Research Team** does that for us."

Sysdig's reporting capabilities have also made a strong impression. The team describes them as some of the most comprehensive and user-friendly that they've encountered, further cementing the platform as an essential part of Automox's security strategy.

> "It's just great technology backed by a great team that wants to partner with their customers in the fight against bad actors."
>
> **Mat Lee**
> Senior Security Engineer, Automox

Actionable Insights and Deep Visibility

With some initial tuning and configuration, Sysdig quickly began delivering actionable, valuable alerts. Instead of wading through countless false positives, Automox's team can now focus their efforts on triaging and resolving genuine threats.

Another transformative benefit has been the unprecedented visibility Sysdig provides into Automox's containers and across their AWS environments.

"With Sysdig, we can see exactly how many of our container images are vulnerable and the specific ways they are at risk," Lee said. "We can also identify in-production vulnerabilities through runtime insights. In fact, we've started building out a dedicated vulnerability management program as a result."

Sysdig has also streamlined the process of reporting vulnerabilities and their impact to leadership. Engineering managers, for instance, can access dashboards with clear, visual breakdowns of container vulnerabilities, and drill down into the potential impact of each issue. This enhanced visibility ensures better communication and more informed decision-making at all levels of the organization, ultimately reducing the attack surface and risk for Automox and its customers.

SOLUTIONS

From Identities to Compliance

"When we first deployed Sysdig we initially saw CSPM as just a 'nice-to-have,' but now we realize how critical it is. Our IAM audit showed that permissions needed review," Lee said. "Sysdig has helped us understand overprovisioned accounts, and it has become a project we are going to tackle this year. We had a feeling that we needed some IAM work, but Sysdig showed us what really had to be done. Having CSPM and threat detection in one place with Sysdig is huge."

Automox is now conducting a comprehensive audit of identities and permissions across all of their cloud service provider accounts – an effort that would require the equivalent of one full-time employee for at least eight weeks if performed manually. With Sysdig, they can access all necessary data through a single pane of glass, significantly streamlining the process.

Sysdig also provides valuable insights into employee activities for both security and auditing purposes. "We're able to create alerts based on high-risk users and their actions," Lee explained. "For instance, we can monitor individuals who might be flight risks or those with extensive access. The logs are then sent to our SIEM for further filtering and analysis."

As Automox works toward achieving and maintaining various compliance standards, Sysdig has become instrumental in building things such as a secure image pipeline. The goal is to have developers operate exclusively from approved repositories, ensuring a more secure and streamlined workflow. Sysdig has also simplified compliance processes by enabling the creation of designated zones where staff can capture screenshots and assess adherence to security standards.

Currently, Automox is in the process of transitioning developers to this new secure pipeline, underscoring their commitment to both operational efficiency and regulatory compliance.

> "We've seen an 80% reduction in security alerts since implementing Sysdig. The platform's precision has significantly improved our threat detection process."
>
> **Mat Lee**
> Senior Security Engineer, Automox

Moving Forward With a Lasting Partnership

For Automox, one of Sysdig's greatest strengths is its exceptional support. Whenever they encounter an issue, such as writing a custom rule, they can count on immediate assistance. Sysdig's Threat Research Team also proactively develops rules to address emerging vulnerabilities, ensuring continuous protection.

A prime example occurred in late March 2024, when a critical vulnerability was discovered in XZ Utils, a widely used data compression software for Linux. Automox quickly initiated triage to assess their exposure and reached out to Sysdig for help crafting a custom rule.

"Sysdig told us they were already on it and would have a new rule ready within an hour or two," Lee said. "That's one of the reasons we value Managed Falco so highly. Managing Falco rules independently – especially in scenarios like this CVE – would be incredibly challenging because of the size of our security team. Sysdig takes that burden off of our shoulders."

This collaborative approach has not only saved Automox countless hours but also positioned Sysdig as a trusted partner in their security journey. Building on this partnership, Automox recently demoed **Sysdig Sage™**, giving them access to an AI-powered cloud security analyst. With Sysdig Sage's advanced capabilities and Sysdig's expert support, Automox continues to enhance their security posture while gaining greater efficiency and peace of mind.

To learn more about Automox, visit **automox.com**.

AUTOMOX

INDUSTRY

Software Technology

INFRASTRUCTURE

Amazon Web Services (AWS)

ORCHESTRATION

Amazon Elastic Kubernetes Service

SOLUTION

Sysdig Secure

About Sysdig

In the cloud, every second counts. Attacks unfold in minutes and security teams must protect the business without slowing it down. Sysdig, named Customers' Choice in the Gartner® "Voice of the Customer" report for cloud-native application protection platforms (CNAPPs), stops cloud attacks in seconds and instantly detects changes in risk with real-time insights and open source Falco. Sysdig Sage™, the industry's first AI cloud security analyst, uplevels human response and enables security, developers, and DevOps to work together, faster. By correlating signals across cloud workloads, identities, and services, Sysdig uncovers hidden attack paths and prioritizes 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 →